APPENDIX

A

Media

IN THIS APPENDIX

Getting Linux distributions

Creating a bootable CD or DVD

Unless you bought a computer with Linux preinstalled or had someone install it for you, you need to find a way to get a Linux distribution and then either install or run it live on your computer. Fortunately, Linux distributions are widely available and come in a variety of forms.

In this appendix, you learn how to do the following:

- Get a few different Linux distributions
- Create a bootable disk to install your distribution
- Boot Linux from a USB drive

To use this book effectively, you should have a Linux distribution in front of you to work on. It's important to be able to experience Linux as you read. So, try the examples and do the exercises.

Linux distributions are most commonly available from the websites of the organizations that produce them. The following sections describe websites associated with Linux distributions that offer ISO images you can download.

NOTE

An ISO is a disk image that is formatted in the ISO 9660 filesystem format, a format that is commonly used with CD and DVD images. Because this is a well-known format, it is readable by Windows, Mac, and Linux systems.

An ISO image can be used to create a bootable USB flash drive, CD, or DVD medium, depending on the size of the image. An ISO image in your filesystem can be mounted in Linux in loopback mode, so you can view or copy its contents.

When an ISO image contains a Linux Live CD or installation image, the images are bootable. This means that instead of starting up an operating system, such as Windows or Linux, from the computer's hard drive, you can tell your computer to boot from the CD or DVD instead. This enables you to run a totally different operating system than is installed on your hard drive without changing or damaging the data on that drive.

Linux® Bible, Tenth Edition. Christopher Negus.

Getting Fedora

NOTE

I recommend downloading the Fedora Workstation Live Image to use along with this book because most of the book works with that distribution. You can run it live without committing to overwriting your computer's hard disk until you feel comfortable enough to install it permanently.

To test the examples in this book, I used Fedora 30 and 31, 64-bit Fedora Workstation images, which you can get from `GetFedora.org` (`https://getfedora.org/en/workstation/download`). If you have a 64-bit machine, you must use the 64-bit ISO.

Later versions of Fedora that come with a GNOME desktop should work as well. Here's a link to the exact ISO used for the Fedora 31 Workstation:

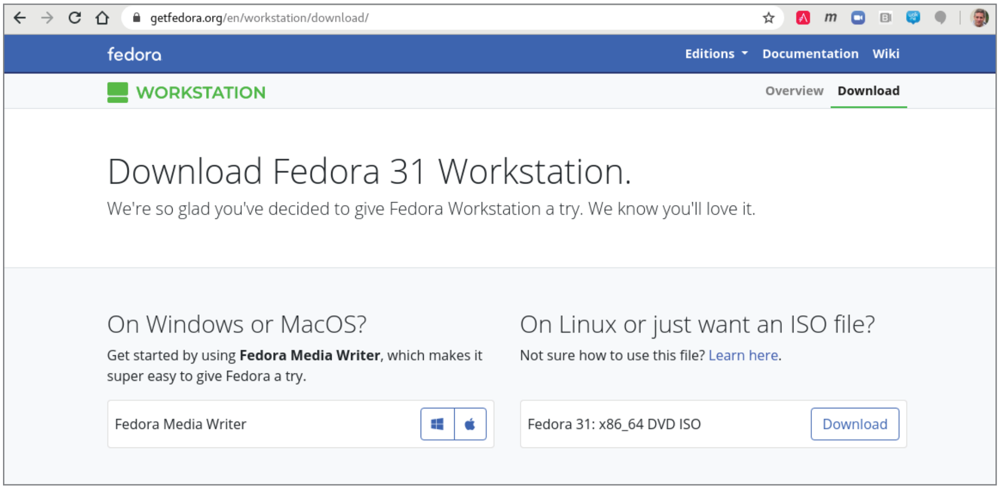
```
https://download.fedoraproject.org/pub/fedora/linux/releases/31/Workstation/
x86_64/iso/Fedora-Workstation-Live-x86_64-31-1.9.iso
```

Keep in mind that the latest Fedora Workstation ISO image does not fit on a CD, so you must burn it to a DVD or USB flash drive. See the descriptions of CD/DVD burning tools available for Windows, MacOS, and Linux later in this appendix.

Figure A.1 shows an example of the Get Fedora page.

FIGURE A.1

Download Fedora ISO images from the Get Fedora page.



Download Fedora 31 Workstation.

We're so glad you've decided to give Fedora Workstation a try. We know you'll love it.

On Windows or MacOS?

Get started by using **Fedora Media Writer**, which makes it super easy to give Fedora a try.

Fedora Media Writer

On Linux or just want an ISO file?

Not sure how to use this file? Learn here.

Fedora 31: x86_64 DVD ISO

Today, the default download is an ISO image of a 64-bit PC-type Fedora Workstation (GNOME) Live DVD. You can boot this image on your computer, and if you choose, you can permanently install it to your computer's hard drive. To download this image, do the following:

1. Select Workstation or Server from `GetFedora.org`. I recommend Workstation to follow along with this book.
2. Select the Download Now button and click the Download button. A pop-up should appear, asking what you want to do with the ISO.
3. Select to save the ISO. Depending on your settings, either you are asked where you want to download it or it simply begins downloading to a default folder (in Linux, it is probably a Downloads folder).
4. If you are prompted for where to put the ISO, select a folder that has enough space to hold it. Remember where this folder is located, because you need to find the ISO when you go to burn it later.

If you need more information about what to do with the downloaded image, there are links to help you on the Fedora page that appears. At the time of this writing, the Learn Here link takes you to descriptions of how to create live installation media. The exact instructions might change as the website is updated.

You have other choices for downloading ISOs from Fedora. From the bottom of the `GetFedora.org` page, you can download specially configured Fedora ISO images called spins (`https://spins.fedoraproject.org`). Here are some special types of Fedora spins that might interest you:

KDE desktop spin: People who prefer the KDE desktop to the GNOME desktop can download the Plasma KDE spin.

Lightweight desktop spin: If you are trying Linux on a computer with less memory or processing power, consider Xfce and LXQt spins (representing lightweight desktops of the same name).

Desktop effects spin: The MATE-Compiz spin offers more of the other extreme to the lightweight desktops, with desktop effects like wobbly windows and desktops that rotate on a cube.

Child-friendly desktop spin: The SOAS desktop is a spin of the Sugar Learning Platform, made to provide a simplified setup and a child-friendly graphical interface. SOAS can be transported on a USB drive and run on any available computer.

Getting Red Hat Enterprise Linux

Many large corporations, government agencies, and universities use Red Hat Enterprise Linux to run their mission-critical applications. While most of the procedures in this book will run well on Fedora, there are many references to how things are done differently in

Red Hat Enterprise Linux because, when you go to get a job as a Linux system administrator, you will, in most cases, be working with Red Hat Enterprise Linux systems.

Although the source code for Red Hat Enterprise Linux is freely available, the ISOs containing the packages you install (often referred to as the *binaries*) are available only to those who have accounts on the Red Hat customer portal (`https://access.redhat.com`) or through evaluation copies.

If you don't have an account, you can try signing up for a 30-day trial. If either you or your company has an account with Red Hat, you can download the ISOs that you need. Go to the following site and follow the instructions to download a Red Hat Enterprise Linux server ISO or sign up to get an evaluation copy:

`https://access.redhat.com/downloads`.

Red Hat does not offer live versions of Red Hat Enterprise Linux. Instead, you can download installation DVDs that you can install as described in Chapter 9, "Installing Linux," of this book.

NOTE

If you are unable to obtain a Red Hat Enterprise Linux installation DVD, you can get a similar experience using the CentOS installation DVD. CentOS is not exactly the same as RHEL. However, if you download the CentOS installation DVD for CentOS 8.x from links on the CentOS site (`http://www.centos.org/download/`), the installation procedure is similar to the one described for Red Hat Enterprise Linux in Chapter 9.

Getting Ubuntu

Many people new to Linux begin by downloading and installing Ubuntu. Ubuntu has a huge fan base and many active contributors. If you have problems with Ubuntu, there are large, active forums where many people are willing to help you overcome problems.

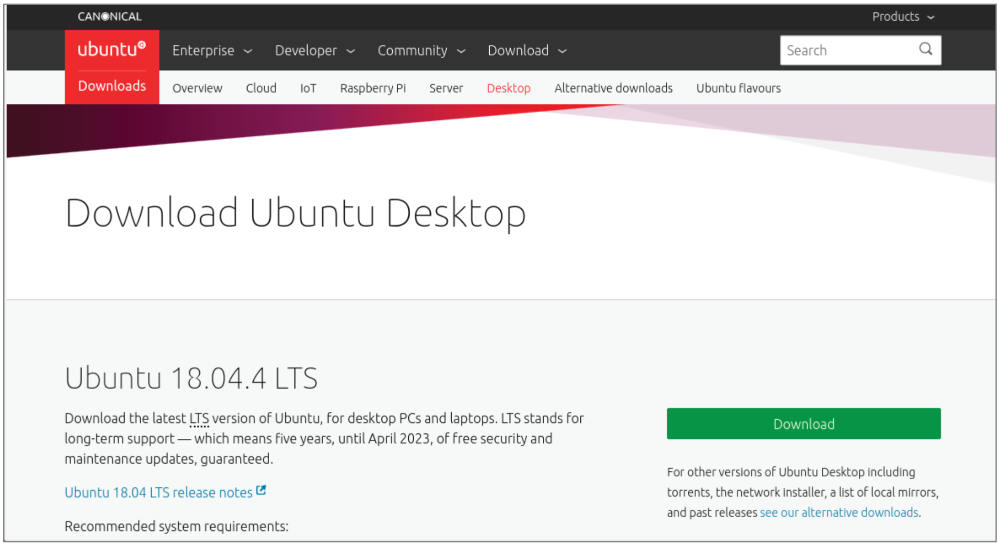
If you already have an Ubuntu system installed, you can follow along with most of this book. You can get Ubuntu with a GNOME desktop, and its default dash shell is similar to bash (or you can switch to bash in Ubuntu to match the shell examples in this book). Although most of the examples of this book focus on Fedora and RHEL, I have added many more references to Ubuntu throughout the book in this edition.

To get Ubuntu, you can download a Live ISO image or installation medium from the Download Ubuntu page: `http://www.ubuntu.com/download/ubuntu`.

Figure A.2 shows an example of the Download Ubuntu Desktop page.

FIGURE A.2

Download Ubuntu Live ISO images, or choose an alternative download.



Download Ubuntu Desktop

Ubuntu 18.04.4 LTS

Download the latest LTS version of Ubuntu, for desktop PCs and laptops. LTS stands for long-term support — which means five years, until April 2023, of free security and maintenance updates, guaranteed.

Ubuntu 18.04 LTS release notes

Recommended system requirements:

For other versions of Ubuntu Desktop including torrents, the network installer, a list of local mirrors, and past releases see our alternative downloads.

As with Fedora, the easiest way to download Ubuntu is to select the 64-bit Ubuntu Live image, download it, and burn it. Here's how to do that from the Download Ubuntu page:

1. Click the Download button. By default, this downloads the most recent 64-bit Ubuntu desktop Live ISO image.
2. Either you are asked where you want to download the ISO image, or it simply begins downloading to a default folder.
3. If you are asked where to put the ISO, select a folder that has enough space to hold the ISO. Remember where this folder is located because you need to find the ISO when you go to burn it later.

After the download is complete, burn the ISO image to a DVD using procedures described in the section "Creating Linux CDs and DVDs".

Other types of Ubuntu installation media are also available. To find other Ubuntu media, go to the Alternative Downloads page (`http://www.ubuntu.com/download/alternative-downloads`). From this site, you can get media that contains a variety of desktop and server installs.

Booting Linux from a USB Drive

Instead of burning ISO images to a CD or DVD, you can put your Linux system on a USB drive. USB drives offer the advantage of being writable as well as readable, so you can save your content between sessions. Most modern computers can boot from a USB drive, although you may have to interrupt the boot process to tell the BIOS to boot from a USB drive instead of hard drive or CD/DVD drive.

You can find procedures for putting Fedora and Ubuntu on a USB drive in the following locations:

Fedora on a USB drive: Using a tool called Live USB Creator, you can install a Fedora ISO image to a USB drive in either Windows or Linux. To run Fedora from that drive, insert it into a USB port on your computer, reboot the computer, interrupt the BIOS as it is booting (possibly F12), and select to boot from a USB drive. The procedure for using Live USB creator is located at

`https://docs.fedoraproject.org/en-US/quick-docs/creating-and-using-a-live-installation-image/index.html`

Ubuntu on a USB drive: Ubuntu has procedures for creating a bootable USB drive with Ubuntu on it that work from Windows, MacOS, or Linux. To find out how to do this, go to the Ubuntu Download page, and under "Easy ways to switch to Ubuntu," look for the appropriate "How to create a bootable USB stick…" procedure for Ubuntu, Windows, or MacOS:

`https://ubuntu.com/tutorials/tutorial-create-a-usb-stick-on-ubuntu#1-overview`

Creating Linux CDs and DVDs

After you have downloaded a Linux CD or DVD image, you can use several tools to create bootable CDs or DVDs for either installing or just running Linux live from those media. Before you begin, you must have the following:

DVD or CD ISO images: Download the ISO images to your computer that represent the physical DVD or CD you will ultimately burn. Today, most Linux ISO images are too big to fit on a CD (including those for RHEL, Fedora, and Ubuntu).

Blank DVDs/CDs: You need blank DVDs or CDs to burn the images to. CDs hold up to about 700MB; DVDs hold up to about 4.7GB (single layer).

CD/DVD burner: You need a drive that is capable of burning CDs or DVDs, depending on which you are burning. Not all CD/DVD drives can burn DVDs (especially older ones). So, you may need to find a computer with a drive that has that capability.

The following sections describe how to burn bootable CDs and DVDs from Windows, MacOS, and Linux systems.

Burning CDs/DVDs in Windows

If you have downloaded your Linux ISO image to a Windows system, you can burn that image to CD or DVD in different ways. Here are some examples:

Windows: In the latest Windows releases, the function of burning ISO images to CD or DVD is built into Windows. After an ISO image is downloaded, simply insert the appropriate CD or DVD into your computer's drive (assuming the drive is writeable), right-click the ISO image icon from the folder to which you downloaded it, and select Burn Disc Image. When the Windows Disc Image Burner window appears, select Burn to burn the image.

Roxio Creator: This third-party Windows application contains many features for ripping and burning CDs and DVDs. You can read about the product here: `http://www.roxio.com/en/products/creator/`.

Nero CD/DVD Burning ROM: Nero is another popular CD/DVD burning software product for Windows systems. You can find out more about Nero here: `http://www.nero.com`.

Burning CDs/DVDs on a MacOS system

Like Windows, MacOS has CD/DVD burning software built into the operating system. To burn an ISO image to disk on a MacOS system, follow these steps:

1. Download the ISO image you want on your MacOS system. An icon representing the ISO should appear on your desktop.
2. Insert a blank CD or DVD into your CD/DVD burner, as appropriate for the size of the image.
3. Right-click the icon representing the Linux ISO that you just downloaded and select Burn "Linux" to Disk. A pop-up window appears, asking if you are sure you want to burn the image.
4. Fill in the name that you want to give the ISO and the write speed and then select Burn. The image begins burning to disk.
5. After the image has been burned, eject the disk; you are ready to boot the CD or DVD on an appropriate computer.

Burning CDs/DVDs in Linux

Linux has both graphical and command-line tools for burning CD and DVD images to physical media. Examples in this section show how to use `K3b` from the desktop or `cdrecord` (or `wodim`) to burn ISO images to CD or DVD. If they are not installed, you can install either one as follows:

For Fedora or RHEL

```
# yum install k3b
# yum install wodim
```

For Debian or Ubuntu

```
# apt-get install k3b
# apt-get install wodim
```

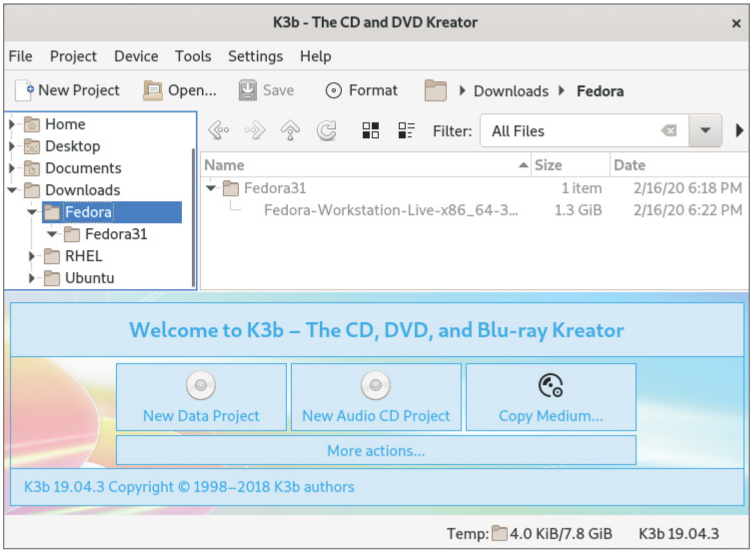
Burning CDs or DVDs from a Linux desktop

Here's how to create bootable Linux CDs or DVDs from a running Linux system (such as Fedora) using `K3b`. `K3b` comes with the KDE desktop but runs on the GNOME desktop as well.

1. Download the ISO images that you want to your computer's hard drive. (A CD image is under about 700MB in size. Single-layer DVD images are under 4.7GB.)
2. Open a CD/DVD burning application. For this procedure, I recommend K3b CD and DVD Kreator (`http://www.k3b.org`). In Fedora, select Activities and type **K3b** (or type **k3b** from a Terminal window). The “K3b – The CD and DVD Kreator” window appears.
3. From the K3b window, select Tools ➪ Burn Image to burn a CD or DVD ISO Image. You are asked to choose an image file.
4. Browse to the image that you just downloaded or copied to hard drive and select it. After you select the image that you want, the Burn Image window appears, as does a checksum on the image. Figure A.3 shows the K3b window ready to select an image of Fedora.

FIGURE A.3

Use K3b to burn your Linux CDs or DVDs.



Name	Size	Date
Fedora31	1 item	2/16/20 6:18 PM
Fedora-Workstation-Live-x86_64-3...	1.3 GiB	2/16/20 6:22 PM

5. Insert a blank CD or DVD into the CD/DVD drive, which may be a combination CD/DVD drive. (If a CD/DVD Creator window pops up, you can close it.)

6. Check the settings in the Burn Image window (often, the defaults are fine, but you may want to slow down the speed if you get some bad burns). You can also select the Simulate check box to test the burn before actually writing to the CD/DVD. Click Start to continue.
7. When the CD/DVD is finished burning, eject it (or it may eject automatically) and mark it appropriately (information such as the distribution name, version number, date, and name of the ISO image).

Now you're ready to begin installing (or booting) the Linux distribution you just burned.

Burning CDs or DVDs from a Linux command line

If you have no GUI, or you don't mind working from the shell, you can use the cdrecord command to burn the ISOs. With a blank CD or DVD inserted and the ISO image you want to burn in the current directory, you can use the following simple command line for burning a CD image to CD or DVD using cdrecord:

```
# cdrecord -v whatever.iso
```

See the cdrecord man page (man cdrecord) for other options available with the cdrecord command.

APPENDIX

B

Exercise Answers

This appendix provides answers to each of the chapter exercises. There are many ways to accomplish tasks in Linux. Suggested answers are provided herein.

Some of the exercises require that you modify system files that could change the basic functioning of your system, or even make your system unbootable. Therefore, I recommend that you do the exercises on a Linux system that you are free to modify and erase if something should go wrong. Using virtual machines, that you can discard when you are done, is an excellent option.

Chapter 1: Starting with Linux

There are no exercises in Chapter 1.

Chapter 2: Creating the Perfect Linux Desktop

This section details some ways that these tasks can be completed on both the GNOME 2 and GNOME 3 desktops.

1. To get started, you need a Linux system in front of you to do the procedures in this book. An installed system is preferable, so you don't lose your changes when you reboot. To start out, you can use a Fedora Live CD (or installed system), an Ubuntu installed system, or a Red Hat Enterprise Linux installed system. Here are your choices:
    a. **Fedora Live CD (GNOME 3):** Get a Fedora Live CD as described in Appendix A. Run it live, as described in the section "Starting with the Fedora GNOME Desktop Live image" in Chapter 2, or install it and run it from hard disk as described in Chapter 9, "Installing Linux."
    b. **Ubuntu (GNOME 3):** Install Ubuntu and the GNOME Shell software, as described at the beginning of Chapter 2.
    c. **Red Hat Enterprise Linux 8 (GNOME 3):** Install Red Hat Enterprise Linux 7, as described in Chapter 9.
    d. **Red Hat Enterprise Linux 6 or earlier (GNOME 2):** Install Red Hat Enterprise Linux 6.

Linux® Bible, Tenth Edition. Christopher Negus.

2. To launch the Firefox web browser and go to the GNOME home page (`http://gnome.org`), there are some easy steps to take. If your network is not working, refer to Chapter 14, "Administering Networking," for help on connecting to wired and wireless networks.

GNOME 3

For GNOME 3, you can press the Windows key to get to the Overview screen. Then type **`Firefox`** to highlight just the Firefox web browser icon. Press Enter to launch it. Type **`http://gnome.org`** in the location box, and press Enter.

GNOME 2

For GNOME 2, select the Firefox icon from the top menu bar. Type **`http://gnome.org`** in the location box, and press Enter.

3. To pick a background that you like from the GNOME art site (`http://gnome-look.org`), download it to your Pictures folder, and select it as your current background. On both GNOME 2 and GNOME 3 systems, do the following:
   a. Type **`http://gnome-look.org/`** in the Firefox location box and press Enter.
   b. Find a background that you like and select it. Then click the Download button and download it to your Pictures folder.
   c. Open your Pictures folder, right-click the image, and select Set as Wallpaper.

      The image is used as your desktop background.

4. To start a Nautilus File Manager window and move it to the second workspace on your desktop, do the following:

For GNOME 3

   a. Press the Windows key.
   b. Select the Files icon from the Dash (left side). A new instance of Nautilus starts in the current workspace.
   c. Right-click the title bar in the Files window and select Move to Monitor Down. The Files window moves to the second workspace.

For GNOME 2

   a. Open the Home folder from the GNOME 2 desktop (double-click).
   b. Right-click in the Nautilus title bar that appears, and select either Move to Workspace Right or Move to Another Workspace. (You can select which workspace you want from the list.)

5. To find the image that you downloaded to use as your desktop background and open it in any image viewer, first go to your Home folder, then open the Pictures folder. Double-click the image to open it in an image viewer.

6. Moving back and forth between the workspace with Firefox on it and the one with the Nautilus file manager is fairly straightforward.

If you did the previous exercises properly, Nautilus and Firefox should be in different workspaces. Here's how you can move between those workspaces in GNOME 3 and GNOME 2:

GNOME 3

Press the Windows key, and select the workspace that you want in the right column. As an alternative, you can go directly to the application that you want by pressing Alt+Tab and pressing Tab again and also arrow keys to highlight the application that you want to open.

GNOME 2

Select the workspace that you want with your mouse by clicking the small representation of the workspace in the right side of the lower panel. If you happen to have Desktop Effects enabled (System ➪ Preferences Desktop Effects ➪ Compiz), try pressing Ctrl+Alt+right arrow (or left arrow) to spin to the next workspace.

7. To open a list of applications installed on your system and select an image viewer to open from that list using as few clicks or keystrokes as possible, do the following:

In GNOME 3

Move the mouse to the upper-left corner of the screen to get to the Overview screen. Select Applications, then select Utilities from the right column, and then select Image Viewer.

In GNOME 2

Select Applications ➪ Graphics ➪ Image Viewer to open an image viewer window on the desktop.

8. To change the view of the windows on your current workspace to smaller views of those windows that you can step through, do the following:

In GNOME 3

With multiple windows open on multiple workspaces, press the Alt+Tab keys. While continuing to hold the Alt key, press Tab until you highlight the application that you want. Release the Alt key to select it.

In GNOME 2

With multiple windows open on multiple workspaces, press and hold the Ctrl+Alt+Tab keys. While continuing to hold the Ctrl+Alt keys, press Tab until you have highlighted the application that you want. Release the Ctrl and Alt keys to select it.

9. To launch a music player from your desktop using only the keyboard, do the following:

In GNOME 3

a. Press the Windows key to go to the Overview screen.

   b. Type **Rhyth** (until the icon appears and is highlighted) and press Enter. (In Ubuntu, if you don't have Rhythmbox installed, type **Bansh** to open the Banshee Media Player.)

In GNOME 2

Press Alt+F2. From the Run Application box that appears. Then type **rhythmbox** and press Enter.

10. To take a picture of your desktop using only keystrokes, press the Print Screen key to take a screen shot of your entire desktop in both GNOME 3 and GNOME 2. Press Alt+Print Screen to take a screen shot of just the current window. In both cases, the images are saved to the Pictures folder in your home folder.

Chapter 3: Using the Shell

1. To switch virtual consoles and return to the desktop in Fedora or Ubuntu (this feature is disabled in some RHEL systems), do the following:
   a. Hold Ctrl+Alt and press F2 (Ctrl+Alt+F2). A text-based console should appear.
   b. Type your username (press Enter) and password (press Enter).
   c. Type a few commands, such as **id**, **pwd**, and **ls**.
   d. Type **exit** to exit the shell and return to the login prompt.
   e. Press Ctrl+Alt+F1 to return to the virtual console that holds your desktop. (On different Linux systems, the desktop may be on different virtual consoles. Ctrl+Alt+F7 and Ctrl+Alt+F2 are other common places to find it.)
2. For your Terminal window, make the font red and the background yellow.
   a. From the GNOME desktop, select Applications ➪ System Tools ➪ Terminal to open a Terminal window.
   b. From the Terminal window, select Edit ➪ Profile Preferences.
   c. Select the Colors tab and deselect "Use colors from system theme" box.
   d. Select the box next to Text Color, click the color red that you want from the available selections, and click Select.
   e. Select the box next to Background Color, click the color yellow that you want from the available selections, and click Select.
   f. Click Close on the Profile window to go back to the Terminal window with the new colors.
   g. Go back and reselect "Use colors from system theme" box to go back to the default Terminal colors.
3. Find the `mount` command and `tracepath` man page.
   a. Run `type mount` to see that the `mount` command's location is either `/usr/bin/mount` or `/bin/mount`.

b. Run `locate tracepath` to see that the `tracepath` man page is at `/usr/share/man/man8/tracepath.8.gz`.

4. Run, recall, and change these commands as described:

```
$ cat /etc/passwd
$ ls $HOME
$ date
```

a. Press the up arrow until you see the `cat /etc/passwd` command. If your cursor is not already at the end of the line, press Ctrl+E to get there. Backspace over the word `passwd`, type the word **group**, and press Enter.

b. Type **man ls**, and find the option to list by time (`-t`). Press the up arrow until you see the `ls $HOME` command. Use the left arrow key or Alt+B to position your cursor to the left of `$HOME`. Type **-t**, so that the line appears as `ls -t $HOME`. Press Enter to run the command.

c. Type **man date** to view the `date` man page. Use the up arrow to recall the `date` command and add the format indicator that you found. A single `%D` format indicator gets the results you need:

```
$ date +%D
04/27/20
```

5. Use tab completion to type **basename /usr/share/doc/**. Type **basen<Tab> /u<Tab>sh<Tab>do<Tab>** to get `basename/usr/share/doc/`.

6. Pipe `/etc/services` to the `less` command: `$ cat /etc/services | less`.

7. Make output from the `date` command appear in this format: Today is Thursday, April 23, 2020.

```
$ echo "Today is $(date +'%A, %B %d, %Y')"
```

8. View variables to find your current hostname, username, shell, and home directories.

```
$ echo $HOSTNAME
$ echo $USERNAME
$ echo $SHELL
$ echo $HOME
```

9. Add a permanent `mypass` alias that displays the contents of the `/etc/passwd` file.

a. Type **nano $HOME/.bashrc**.

b. Move the cursor to an open line at the bottom of the page. (Press Enter to open a new line if needed.)

c. On its own line, type **alias m="cat /etc/passwd"**.

d. Type Ctrl+O to save and Ctrl+X to exit the file.

e. Type **source $HOME/.bashrc**.

   f. Type **alias m** to make sure that the alias was set properly: alias m='cat /etc/passwd'.

   g. Type **m**. (The /etc/passwd file displays on the screen.)

10. To display the man page for the mount system call, use the man -k command to find man pages that include the word mount. Then use the mount command with the correct section number (8) to get the proper mount man page:

```
        $ man -k mount | grep ^mount
        mount       (2)  - mount filesystem
        mount       (8)  - mount a filesystem
        ...
        mountpoint  (1)  - see if a directory is a mountpoint
        mountstats  (8)  - Displays various NFS client per-mount
statistics
        $ man 2 mount
        MOUNT(2)      Linux Programmer's Manual
MOUNT(2)
        NAME
              mount - mount file system
        SYNOPSIS
              #include <sys/mount.h>
.
.
.
```

Chapter 4: Moving Around the Filesystem

1. Create the projects directory, create nine empty files (house1 to house9), and list just those files.

```
$ mkdir $HOME/projects/
$ touch $HOME/projects/house{1..9}
$ ls $HOME/projects/house{1..9}
```

2. Make the $HOME/projects/houses/doors/ directory path, and create some empty files in that path.

```
$ cd
$ mkdir $HOME/projects/houses
$ touch $HOME/projects/houses/bungalow.txt
$ mkdir $HOME/projects/houses/doors/
$ touch $HOME/projects/houses/doors/bifold.txt
$ mkdir -p $HOME/projects/outdoors/vegetation/
$ touch $HOME/projects/outdoors/vegetation/landscape.txt
```

3. Copy the files house1 and house5 to the $HOME/projects/houses/ directory.

```
$ cp $HOME/projects/house[15] $HOME/projects/houses
```

4. Recursively copy the /usr/share/doc/initscripts* directory to the $HOME/projects/ directory.

```
$ cp -ra /usr/share/doc/initscripts*/ $HOME/projects/
```

5. Recursively list the contents of the $HOME/projects/ directory. Pipe the output to the less command so that you can page through the output.

```
$ ls -lR $HOME/projects/ | less
```

6. Remove the files house6, house7, and house8 without being prompted.

```
$ rm -f $HOME/projects/house[678]
```

7. Move house3 and house4 to the $HOME/projects/houses/doors directory.

```
$ mv $HOME/projects/house{3,4} $HOME/projects/houses/doors/
```

8. Remove the $HOME/projects/houses/doors directory and its contents.

```
$ rm -rf $HOME/projects/houses/doors/
```

9. Change the permissions on the $HOME/projects/house2 file so that it can be read and written to by the user who owns the file, only read by the group, and have no permission for others.

```
$ chmod 640 $HOME/projects/house2
```

10. Recursively change the permissions of the $HOME/projects/ directory so that nobody has write permission to any files or directories beneath that point in the file system.

```
$ chmod -R a-w $HOME/projects/
$ ls -lR $HOME/projects/
/home/joe/projects/:

total 12

-r--r--r--. 1 joe joe    0 Jan 16 06:49 house1

-r--r-----. 1 joe joe    0 Jan 16 06:49 house2

-r--r--r--. 1 joe joe    0 Jan 16 06:49 house5

-r--r--r--. 1 joe joe    0 Jan 16 06:49 house9

dr-xr-xr-x. 2 joe joe 4096 Jan 16 06:57 houses

dr-xr-xr-x. 2 joe joe 4096 Jul  1  2014 initscripts-9.03.40

dr-xr-xr-x. 3 joe joe 4096 Jan 16 06:53 outdoors
...
```

Chapter 5: Working with Text Files

1. Follow these steps to create the /tmp/services file, and then edit it so that WorldWideWeb appears as World Wide Web.

   ```
   $ cp /etc/services /tmp
   $ vi /tmp/services
   /WorldWideWeb<Enter>
   cwWorld Wide Web<Esc>
   ```

   The next two lines show the before and after:

   ```
   http            80/tcp     www www-http    # WorldWideWeb HTTP
   http            80/tcp     www www-http    # World Wide Web HTTP
   ```

2. One way to move the paragraph in your /tmp/services file is to search for the first line of the paragraph, delete five lines (5dd), go to the end of the file (G), and put in the text (p):

   ```
   $ vi /tmp/services
   /Note that it is<Enter>
   5dd
   G
   p
   ```

3. To use ex mode to search for every occurrence of the term tcp (case sensitive) in your /tmp/services file, and change it to WHATEVER, you can enter the following:

   ```
   $ vi /tmp/services
   :g/tcp/s//WHATEVER/g<Enter>
   ```

4. To search the /etc directory for every file named passwd and redirect errors from your search to /dev/null, you can enter the following:

   ```
   $ find /etc -name passwd 2> /dev/null
   ```

5. Create a directory in your home directory called TEST. Create files in that directory named one, two, and three that have full read/write/execute permissions on for everyone (user, group, and other). Construct a find command that would find those files and any other files that have write permission open to “others” from your home directory and below.

   ```
   $ mkdir $HOME/TEST
   $ touch $HOME/TEST/{one,two,three}
   $ chmod 777 $HOME/TEST/{one,two,three}
   $ find $HOME -perm -002 -type f -ls
   148120  0 -rwxrwxrwx   1 chris chris 0 Jan  1 08:56 /home/
   chris/TEST/two
   ```

```
       148918  0 -rwxrwxrwx   1 chris chris 0 Jan  1 08:56 home/chris/
TEST/three
       147306  0 -rwxrwxrwx   1 chris chris 0 Jan  1 08:56 /home/chris/
TEST/one
```

6. Find files under the /usr/share/doc directory that have not been modified in more than 300 days.

```
$ find /usr/share/doc -mtime +300
```

7. Create a /tmp/FILES directory. Find all files under the /usr/share directory that are more than 5MB and less than 10MB, and copy them to the /tmp/FILES directory.

```
$ mkdir /tmp/FILES
$ find /usr/share -size +5M -size -10M -exec cp {} /tmp/FILES \;
$ du -sh /tmp/FILES/*
6.6M    /tmp/FILES/BidiCharacterTest.txt
7.6M    /tmp/FILES/BidiTest.txt
5.2M    /tmp/FILES/day.jpg
```

8. Find every file in the /tmp/FILES directory, and make a backup copy of each file in the same directory. Use each file's existing name and append .mybackup to create each backup file.

```
$ find /tmp/FILES/ -type f -exec cp {} {}.mybackup \;
```

9. Install the kernel-doc package in Fedora or Red Hat Enterprise Linux. Using grep, search inside the files contained in the /usr/share/doc/kernel-doc* directory for the term e1000 (case insensitive), and list the names of the files that contain that term.

```
# yum install kernel-doc
$ cd /usr/share/doc/kernel-doc*
$ grep -rli e1000 .
./Documentation/powerpc/booting-without-of.txt
./Documentation/networking/e100.txt
...
```

10. Search for the e1000 term again in the same location. However, this time list every line that contains the term and highlight the term in color.

```
$ cd /usr/share/doc/kernel-doc-*
$ grep -ri --color e1000 .
```

Chapter 6: Managing Running Processes

1. To list all processes running on your system with a full set of columns, while piping the output to less, enter the following:

```
$ ps -ef | less
```

2. To list all processes running on the system and sort those processes by the name of the user running each process, enter the following:

```
$ ps -ef --sort=user | less
```

3. To list all processes running on the system with the column names process ID, username, group name, nice value, virtual memory size, resident memory size, and command, enter the following:

```
$ ps -eo 'pid,user,group,nice,vsz,rss,comm' | less
  PID USER     GROUP     NI    VSZ   RSS COMMAND
    1 root     root       0  19324  1236 init
    2 root     root       0      0     0 kthreadd
    3 root     root       -      0     0 migration/0
    4 root     root       0      0     0 ksoftirqd/0
```

4. To run the `top` command and then go back and forth between sorting by CPU usage and memory consumption, enter the following:

```
$ top
P
M
P
M
```

5. To start the `gedit` process from your desktop and use the System Monitor window to kill that process, do the following:

```
$ gedit &
```

Next, in GNOME 2, select Applications ➪ System Tools ➪ System Monitor, or in GNOME 3, from the Activities screen, type **System Monitor** and press Enter. Find the `gedit` process on the Processes tab. (You can sort alphabetically to make it easier by clicking the Process Name heading.) Right-click the `gedit` command, and then select either End Process or Kill Process; the `gedit` window on your screen should disappear.

6. To run the `gedit` process and use the `kill` command to send a signal to pause (stop) that process, enter the following:

```
$ gedit &
[1] 21532

$ kill -SIGSTOP 21532
```

7. To use the `killall` command to tell the `gedit` command (paused in the previous exercise) to continue working, do the following:

```
$ killall -SIGCONT gedit
```

Make sure that the text you typed after `gedit` was paused now appears in the window.

8. To install the xeyes command, run it about 20 times in the background, and run killall to kill all 20 xeyes processes at once, enter the following:

```
# yum install xorg-x11-apps
$ xeyes &
$ xeyes &
...
$ killall xeyes &
```

   Remember, you need to be the root user to install the package. After that, remember to repeat the xeyes command 20 times. Spread the windows around on your screen, and move the mouse for fun to watch the eyes move. All the xeyes windows should disappear at once when you type killall xeyes.

9. As a regular user, run the gedit command so that it starts with a nice value of 5.

```
# nice -n 5 gedit &
[1] 21578
```

10. To use the renice command to change the nice value of the gedit command you just started to 7, enter the following:

```
# renice -n 7 21578
21578: old priority 0, new priority 7
```

   Use any command you like to verify that the current nice value for the gedit command is now set to 7. For example, you could type the following:

```
# ps -eo 'pid,user,nice,comm' | grep gedit
21578 chris     7 gedit
```

Chapter 7: Writing Simple Shell Scripts

1. Here's an example of how to create a script in your $HOME/bin directory called myownscript. When the script runs, it should output information that appears as follows:

```
Today is Sat Jun 10 15:45:04 EDT 2019.
You are in /home/joe and your host is abc.example.com.
```

   The following steps show one way to create the script named myownscript:

   a. If it doesn't already exist, create a bin directory:

```
$ mkdir $HOME/bin
```

   b. Using any text editor, create a script called $HOME/bin/myownscript that contains the following:

```
#!/bin/bash
# myownscript
# List some information about your current system
```

```
          echo "Today is $(date)."
          echo "You are in $(pwd) and your host is $(hostname)."
```

c. Make the script executable:

```
          $ chmod 755 $HOME/bin/myownscript
```

2. Create a script that reads in three positional parameters from the command line, assigns those parameters to variables named ONE, TWO, and THREE, respectively. Also, replace X with the number of parameters and Y with all of the parameters entered. Then replace A with the contents of variable ONE, B with variable TWO, and C with variable THREE, as shown below:

   a. To create the script, open a file named $HOME/bin/myposition and add the following contents:

```
#!/bin/bash
# myposition
ONE=$1
TWO=$2
THREE=$3
echo "There are $# parameters that include: $@"
echo "The first is $ONE, the second is $TWO, the third is
$THREE."
```

   b. To make the script called $HOME/bin/myposition executable, enter the following:

```
          $ chmod 755 $HOME/bin/myposition
```

   c. To test it, run it with some command-line arguments, as in the following:

```
$ myposition Where Is My Hat Buddy?
There are 5 parameters that include: Where Is My Hat Buddy?
The first is Where, the second is Is, the third is My.
```

3. To create the script described, do the following:

   a. To create a file called $HOME/bin/myhome and make it executable, enter the following:

```
          $ touch $HOME/bin/myhome
          $ chmod 755 $HOME/bin/myhome
```

   b. Here's what the script myhome might look like:

```
          #!/bin/bash
          # myhome
          read -p "What street did you grow up on? " mystreet
          read -p "What town did you grow up in? " mytown
          echo "The street I grew up on was $mystreet and the town
  was $mytown."
```

c. Run the script to check that it works. The following example shows what the input and output for the script could look like:

```
$ myhome
What street did you grow up on? Harrison
What town did you grow up in? Princeton
The street I grew up on was Harrison and the town was Princeton.
```

4. To create the required script, do the following:

   a. Using any text editor, create a script called $HOME/bin/myos and make the script executable:

```
$ touch $HOME/bin/myos
$ chmod 755 $HOME/bin/myos
```

   b. The script could contain the following:

```
        #!/bin/bash
        # myos
        read -p "What is your favorite operating system, Mac,
Windows or Linux? " opsys
        if [ $opsys = Mac ] ; then
          echo "Mac is nice, but not tough enough for me."
        elif [ $opsys = Windows ] ; then
          echo "I used Windows once. What is that blue screen
for?"
        elif [ $opsys = Linux ] ; then
          echo "Great Choice!"
        else
          echo "Is $opsys an operating system?"
        fi
```

5. To create a script named $HOME/bin/animals that runs through the words *moose*, *cow*, *goose*, and *sow* through a for loop and have each of those words appended to the end of the line "I have a. . .," do the following:

   a. Make the script executable:

```
$ touch $HOME/bin/animals
$ chmod 755 $HOME/bin/animals
```

   b. The script could contain the following:

```
#!/bin/bash
# animals
for ANIMALS in moose cow goose sow ; do
  echo "I have a $ANIMALS"
done
```

   c. When you run the script, the output should appear as follows:

```
$ animals
I have a moose
```

```
I have a cow
I have a goose
I have a sow
```

Chapter 8: Learning System Administration

1. To enable Cockpit on your system, enter the following:

   ```
   # systemctl enable --now cockpit.socket
   Created symlink /etc/systemd/system/sockets.target.wants/
   cockpit.socket
      → /usr/lib/systemd/system/cockpit.socket
   ```

2. To open the Cockpit interface in your web browser, enter the hostname or IP address of the system holding your Cockpit service, followed by port number 9090. For example, enter this into the location box of your browser:

   ```
   https://host1.example.com:9090/
   ```

3. To find all of the files under the /var/spool directory that are owned by users other than root and do a long listing of them, enter the following. (I recommend becoming root to find files that might be closed off to other users.)

   ```
   $ su -
   Password: *********
   # find /var/spool -not -user root -ls | less
   ```

4. To become root user and create an empty or plain-text file named /mnt/test.txt, enter the following:

   ```
   $ su -
   Password: *********
   # touch /mnt/test.txt
   # ls -l /mnt/test.txt
   -rw-r--r--. 1 root root 0 Jan  9 21:51 /mnt/test.txt
   ```

5. To become root and edit the /etc/sudoers file to allow your regular user account (for example, bill) to have full root privilege via the sudo command, do the following:

   ```
   $ su -
   Password: *********
   # visudo
   o
   bill     ALL=(ALL)     ALL
   Esc ZZ
   ```

   Because visudo opens the /etc/sudoers file in vi, the example types o to open a line, and then it types in the line to allow bill to have full root privilege.

After the line is typed, press Esc to return to command mode and type **ZZ** to write and quit.

6. To use the sudo command to create a file called /mnt/test2.txt and verify that the file is there and owned by the root user, enter the following:

```
[bill]$ sudo touch /mnt/test2.txt
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.
[sudo] password for bill:  *********
[bill]$ ls -l /mnt/text2.txt
-rw-r--r--. 1 root root 0 Jan  9 23:37 /mnt/text2.txt
```

7. Do the following to mount and unmount a USB drive and watch the system journal during this process:

   a. Run the journalctl -f command as root in a Terminal window and watch the output from here for the next few steps.

```
# journalctl -f
Jan 25 16:07:59 host2 kernel: usb 1-1.1: new high-speed USB device
    number 16 using ehci-pci
Jan 25 16:07:59 host2 kernel: usb 1-1.1: New USB device found,
    idVendor=0ea0, idProduct=2168
Jan 25 16:07:59 host2 kernel: usb 1-1.1: New USB device strings:
    Mfr=1, Product=2, SerialNumber=3
Jan 25 16:07:59 host2 kernel: usb 1-1.1: Product: Flash Disk
Jan 25 16:07:59 host2 kernel: usb 1-1.1: Manufacturer: USB
...
Jan 25 16:08:01 host2 kernel: sd 18:0:0:0: [sdb] Write Protect is off
Jan 25 16:08:01 host2 kernel: sd 18:0:0:0: [sdb]
    Assuming drive cache: write through
Jan 25 16:08:01 host2 kernel:  sdb: sdb1
Jan 25 16:08:01 host2 kernel: sd 18:0:0:0: [sdb]
    Attached SCSI removable disk
```

   b. Plug in a USB storage drive that mounts a filesystem from that drive automatically. If it does not, run the following commands in a second terminal (as root) to create a mount point directory and mount the device:

```
$ mkdir /mnt/test
$ mount /dev/sdb1 /mnt/test
$ umount /dev/sdb1
```

8. To see what USB devices are connected to your computer, enter the following:

```
$ lsusb
```

9. To load the bttv module, list the modules that were loaded, and unload it, enter the following:

```
# modprobe -a bttv
# lsmod | grep bttv
ttv                  167936  0
tea575x                16384  1 bttv
tveeprom               28672  1 bttv
videobuf_dma_sg        24576  1 bttv
videobuf_core          32768  2 videobuf_dma_sg,bttv
v4l2_common            16384  1 bttv
videodev              233472  3 tea575x,v4l2_common,bttv
i2c_algo_bit           16384  1 bttv
```

Notice that other modules (v4l2_common, videodev, and others) were loaded when you loaded bttv with modprobe -a.

10. Enter the following to remove the bttv module along with any other modules that were loaded with it. Notice that they were all gone after running modprobe -r.

```
# modprobe -r bttv
# lsmod | grep bttv
```

Chapter 9: Installing Linux

1. To install a Fedora system from Fedora Live media, follow the instructions in the section "Installing Fedora from Live Media" in Chapter 9. In general, those steps include the following:

   a. Booting the Live media.

   b. Selecting to install to the hard drive when the system boots up.

   c. Adding information from the summary page needed to configure your system initially.

   d. Rebooting your computer and removing the Live medium so that the newly installed system boots from the hard drive.

2. To update the packages, after the Fedora Live media installation is complete, do the following:

   a. Reboot the computer and fill in the first boot questions as prompted.

   b. Using a wired or wireless connection, make sure that you have a connection to the Internet. Refer to Chapter 14, "Administering Networking," if you have trouble getting your networking connection to work properly. Open a shell as the root user and type **sudo dnf update**.

   c. When prompted, type **y** to accept the list of packages displayed. The system begins downloading and installing the packages.

3. To run the RHEL installation in text mode, do the following:
   a. Boot the RHEL DVD.
   b. When you see the boot menu, highlight one of the installation boot entries and press Tab. Move the cursor right to the end of the kernel line, and type the literal option **`text`** at the end of that line. Press Enter to start the installer.
   c. Try out the rest of the installation in text mode.
4. To set the disk partitioning as described in question 4 for a Red Hat Enterprise Linux DVD installation, do the following:

NOTE

This procedure ultimately deletes all content on your hard disk. If you just want to use this exercise to practice partitioning, you can reboot your computer before starting the actual installation process without harming your hard disk. After you go forward and partition your disk, assume that all data has been deleted.

   a. On a computer that you can erase with at least 10GB of disk space, insert a RHEL installation DVD, reboot, and begin stepping through the installation screens.
   b. When you get to the Installation Summary screen, select Installation Destination.
   c. From the Installation Destination screen, select the device to use for the installation (probably `sda` if you have a single hard disk that you can completely erase or `vda` for a virtual install).
   d. Select the Custom button.
   e. Select Done to get to the Manual Partitioning screen.
   f. If the existing disk space is already consumed, you need to delete the partitions before proceeding.
   g. Click the plus (+) button at the bottom of the screen. Then add each of the following mount points:

```
/boot - 400M

/  -  3G

/var - 2G

/home  -2G
```

   h. Select Done. You should see a summary of changes.
   i. If the changes look acceptable, select Accept Changes. If you are just practicing and don't actually want to change your partitions, select Cancel & Return to Custom Partitioning. Then simply exit the installer.

Chapter 10: Getting and Managing Software

1. To search the YUM repository for the package that provides the mogrify command, enter the following:

```
# yum provides mogrify
```

2. To display information about the package that provides the mogrify command and determine what is that package's home page (URL), enter the following:

```
# yum info ImageMagick
```

   You will see that the URL to the home page for ImageMagick is http://www.imagemagick.org.

3. To install the package containing the mogrify command, enter the following:

```
# yum install ImageMagick
```

4. To list all of the documentation files contained in the package that provides the mogrify command, enter the following:

```
# rpm -qd ImageMagick
...
/usr/share/doc/ImageMagick/README.txt
...
/usr/share/man/man1/identify.1.gz
/usr/share/man/man1/import.1.gz
/usr/share/man/man1/mogrify.1.gz
```

5. To look through the change log of the package that provides the mogrify command, enter the following:

```
# rpm -q --changelog ImageMagick | less
```

6. To delete the mogrify command from your system and verify its package against the RPM database to see that the command is indeed missing, enter the following:

```
# type mogrify
mogrify is /usr/bin/mogrify
# rm /usr/bin/mogrify
rm remove regular file '/usr/bin/mogrify'? y
# rpm -V ImageMagick
missing   /usr/bin/mogrify
```

7. To reinstall the package that provides the mogrify command and make sure that the entire package is intact again, enter the following:

```
# yum reinstall ImageMagick
# rpm -V ImageMagick
```

8. To download the package that provides the mogrify command to your current directory, enter the following:

```
# yum download ImageMagick
ImageMagick-6.9.10.28-1.fc30.x86_64.rpm
```

9. To display general information about the package that you just downloaded by querying the package's RPM file in the current directory, enter the following:

```
# rpm -qip ImageMagick-6.9.10.28-1.fc30.x86_64.rpm
Name        : ImageMagick
Epoch       : 1
Version     : 6.9.10.28
Release     : 1.fc30



...
```

10. To remove the package containing the mogrify command from your system, enter the following:

```
# yum remove ImageMagick
```

Chapter 11: Managing User Accounts

For questions that involve adding and removing user accounts, you can use the Users window, the User Manager window, or command-line tools such as useradd and usermod. The point is to make sure that you get the correct results shown in the answers that follow, not necessarily to do it exactly in the same way that I did.

There are multiple ways that you can achieve the same results. The answers here show how to complete the exercises from the command line. (Become root user when you see a # prompt.)

1. To add a local user account to your Linux system that has a username of jbaxter and a full name of John Baxter, which uses /bin/sh as its default shell and is the next available UID (yours may differ from the one shown here), enter the following. You can use the grep command to check the new user account. Then set the password for jbaxter to: My1N1te0ut!

```
# useradd -c "John Baxter" -s /bin/sh jbaxter
# grep jbaxter /etc/passwd
jbaxter:x:1001:1001:John Baxter:/home/jbaxter:/bin/sh
# passwd jbaxter
Changing password for user jbaxter
New password: My1N1te0ut!
Retype new password: My1N1te0ut!
passwd: all authentication tokens updated successfully
```

2. To create a group account named testing that uses group ID 315, enter the following:

```
# groupadd -g 315 testing
# grep testing /etc/group
testing:x:315:
```

3. To add jbaxter to the testing group and the bin group, enter the following:

```
# usermod -aG testing,bin jbaxter
# grep jbaxter /etc/group
bin:x:1:bin,daemon,jbaxter
jbaxter:x:1001:
testing:x:315:jbaxter
```

4. To become jbaxter and temporarily have the testing group be jbaxter's default group, run touch /home/jbaxter/file.txt so that the testing group is assigned as the file's group, and do the following:

```
        $ su - jbaxter
        Password: My1N1te0ut!
        sh-4.2$ newgrp testing
        sh-4.2$ touch /home/jbaxter/file.txt
        sh-4.2$ ls -l /home/baxter/file.txt
        -rw-rw-r--. 1 jbaxter testing 0 Jan 25 06:42 /home/jbaxter/file.
txt
        sh-4.2$ exit ; exit
```

5. Note what user ID has been assigned to jbaxter, and then delete the user account without deleting the home directory assigned to jbaxter.

```
$ userdel jbaxter
```

6. Use the following command to find any files in the /home directory (and any subdirectories) that are assigned to the user ID that recently belonged to the user named jbaxter. (When I did it, the UID/GID were both 1001; yours may differ.) Notice that the username jbaxter is no longer assigned on the system, so any files that user created are listed as belonging to UID 1001 and GID 1001, except for a couple of files that were assigned to the testing group because of the newgrp command run earlier:

```
        # find /home -uid 1001 -ls
        262184  4 drwx------ 4 1001  1001  4096 Jan 25 08:00 /home/
jbaxter
        262193  4 -rw-r--r-- 1 1001  1001   176 Jan 27  2011 /home/
jbaxter/.bash_profile
        262196  4 -rw------- 1 13602 testing 93 Jan 25 08:00 /home/
jbaxter/.bash_history
        262194  0 -rw-rw-r-- 1 13602 testing  0 Jan 25 07:59 /home/
jbaxter/file.txt
        ...
```

7. Run these commands to copy the /etc/services file to the /etc/skel/ directory; then add a new user to the system named mjones, with a full name of Mary Jones and a home directory of /home/maryjones. List her home directory to make sure that the services file is there.

```
# cp /etc/services /etc/skel/
# useradd -d /home/maryjones -c "Mary Jones" mjones
```

```
        # ls -l /home/maryjones
        total 628
        -rw-r--r--. 1 mjones mjones 640999 Jan 25 06:27 services
```

8. Run the following command to find all files under the /home directory that belong to mjones. If you did the exercises in order, notice that after you deleted the user with the highest user ID and group ID, those numbers were assigned to mjones. As a result, any files left on the system by jbaxter now belong to mjones. (For this reason, you should remove or change ownership of files left behind when you delete a user.)

```
        # find /home -user mjones -ls
        262184 4 drwx------ 4 mjones mjones 4096 Jan 25 08:00 /
home/jbaxter
        262193 4 -rw-r--r-- 1 mjones mjones 176 Jan 27 2011 /home/
jbaxter/.bash_profile
        262189 4 -rw-r--r-- 1 mjones mjones 18 Jan 27 2011 /home/
jbaxter/.bash_logout
        262194 0 -rw-rw-r-- 1 mjones testing 0 Jan 25 07:59 /home/
jbaxter/file.txt
        262188 4 -rw-r--r-- 1 mjones mjones 124 Jan 27 2011 /home/
jbaxter/.bashrc
        262197 4 drwx------ 4 mjones  mjones 4096 Jan 25 08:27 /
home/maryjones
        262207 4 -rw-r--r-- 1 mjones mjones 176 Jan 27 2011 /home/
maryjones/.bash_profile
        262202 4 -rw-r--r-- 1 mjones mjones 18 Jan 27 2011 /home/
maryjones/.bash_logout
        262206 628 -rw-r--r-- 1 mjones mjones 640999 Jan 25 08:27 /
home/maryjones/services
        262201 4 -rw-r--r-- 1 mjones mjones 124 Jan 27 2011 /home/
maryjones/.bashrc
```

9. As the user mjones, you can use the following to create a file called /tmp/maryfile.txt, and use ACLs to assign the bin user read/write permission and the lp group read/write permission to that file.

```
        [mjones]$ touch /tmp/maryfile.txt
        [mjones]$ setfacl -m u:bin:rw /tmp/maryfile.txt
        [mjones]$ setfacl -m g:lp:rw /tmp/maryfile.txt
        [mjones]$ getfacl /tmp/maryfile.txt
        # file: tmp/maryfile.txt
        # owner: mjones
        # group: mjones
        user::rw-
        user:bin:rw-
        group::rw-
        group:lp:rw-
        mask::rw-
        other::r& —
```

10. Run this set of commands (as mjones) to create a directory named /tmp/mydir, and use ACLs to assign default permissions to it so that the adm user has read/write/execute permission to that directory and any files or directories created in it. Test that it worked by creating the /tmp/mydir/testing/ directory and /tmp/mydir/newfile.txt.

```
[mary]$ mkdir /tmp/mydir
[mary]$ setfacl -m d:u:adm:rwx /tmp/mydir
[mjones]$ getfacl /tmp/mydir
# file: tmp/mydir
# owner: mjones
# group: mjones
user::rwx
group::rwx
other::r-x
default:user::rwx
default:user:adm:rwx
default:group::rwx
default:mask::rwx
default:other::r-x
[mjones]$ mkdir /tmp/mydir/testing
[mjones]$ touch /tmp/mydir/newfile.txt
[mjones]$ getfacl /tmp/mydir/testing/
# file: tmp/mydir/testing/
# owner: mjones
# group: mjones
user::rwx
user:adm:rwx
group::rwx
mask::rwx
other::r-x
default:user::rwx
default:user:adm:rwx
default:group::rwx
default:mask::rwx
default:other::r-x
[mjones]$ getfacl /tmp/mydir/newfile.txt
# file: tmp/mydir/newfile.txt
# owner: mjones
# group: mjones
user::rw-
user:adm:rwx     #effective:rw-
group::rwx       #effective:rw-
mask::rw-
other::r--
```

Notice that the adm user effectively has only rw- permission. To remedy that, you need to expand the permissions of the mask. One way to do that is with the chmod command, as follows:

```
[mjones]$ chmod 775 /tmp/mydir/newfile.txt
[mjones]$ getfacl /tmp/mydir/newfile.txt
# file: tmp/mydir/newfile.txt
# owner: mjones
# group: mjones
user::rwx
user:adm:rwx
group::rwx
mask::rwx
other::r-x
```

Chapter 12: Managing Disks and Filesystems

1. To determine the device name of a USB flash drive that you want to insert into your computer, enter the following and insert the USB flash drive. (Press Ctrl+C after you have seen the appropriate messages.)

```
# journalctl -f
kernel: [sdb] 15667200 512-byte logical blocks:
     (8.02 GB/7.47 GiB)
Feb 11 21:55:59 cnegus kernel: sd 7:0:0:0:
     [sdb] Write Protect is off
Feb 11 21:55:59 cnegus kernel: [sdb] Assuming
     drive cache: write through
Feb 11 21:55:59 cnegus kernel: [sdb] Assuming
     drive cache: write through
```

2. To list partitions on the USB flash drive on a RHEL 6 system, enter the following:

```
# fdisk -c -u -l /dev/sdb
```

   To list partitions on a RHEL 7, RHEL 8, or Fedora system, enter the following:

```
# fdisk -l /dev/sdb
```

3. To delete partitions on the USB flash drive, assuming device /dev/sdb, do the following:

```
# fdisk /dev/sdb
Command (m for help): d
Partition number (1-6): 6
Command (m for help): d
Partition number (1-5): 5
Command (m for help): d
```

```
Partition number (1-5): 4
Command (m for help): d
Partition number (1-4): 3
Command (m for help): d
Partition number (1-4): 2
Command (m for help): d
Selected partition 1
Command (m for help): w
# partprobe /dev/sdb
```

4. To add a 100MB Linux partition, 200MB swap partition, and 500MB LVM partition to the USB flash drive, enter the following:

```
# fdisk /dev/sdb

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First sector (2048-15667199, default 2048):  <ENTER>
Last sector, +sectors or +size{K,M,G} (default 15667199): +100M
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 2
First sector (616448-8342527, default 616448):  <ENTER>
Last sector, +sectors or +size{K,M,G} (default 15667199): +200M
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First sector (616448-15667199, default 616448):  <ENTER>
Using default value 616448
Last sector, +sectors or +size{K,M,G} (default 15667199): +500M
Command (m for help): t
Partition number (1-4): 2
Hex code (type L to list codes): 82
Changed system type of partition 2 to 82 (Linux swap / Solaris)
Command (m for help): t
Partition number (1-4): 3
Hex code (type L to list codes): 8e
Changed system type of partition 3 to 8e (Linux LVM)
```

```
Command (m for help): w
# partprobe /dev/sdb
# grep sdb /proc/partitions
   8       16    7833600 sdb
   8       17     102400 sdb1
   8       18     204800 sdb2
   8       19     512000 sdb3
```

5. To put an ext4 filesystem on the Linux partition, enter the following:

```
# mkfs -t ext4 /dev/sdb1
```

6. To create a mount point called /mnt/mypart and mount the Linux partition on it, do the following:

```
# mkdir /mnt/mypart
# mount -t ext4 /dev/sdb1 /mnt/mypart
```

7. To enable the swap partition and turn it on so that additional swap space is immediately available, enter the following:

```
# mkswap /dev/sdb2
# swapon /dev/sdb2
```

8. To create a volume group called abc from the LVM partition, create a 200MB logical volume from that group called data, create a VFAT filesystem on it, temporarily mount the logical volume on a new directory named /mnt/test, and then check that it was successfully mounted, enter the following:

```
# pvcreate /dev/sdb3
# vgcreate abc /dev/sdb3
# lvcreate -n data -L 200M abc
# mkfs -t vfat /dev/mapper/abc-data
# mkdir /mnt/test
# mount /dev/mapper/abc-data /mnt/test
```

9. To grow the logical volume from 200MB to 300MB, enter the following:

```
# lvextend -L +100M /dev/mapper/abc-data
# resize2fs -p /dev/mapper/abc-data
```

10. To remove the USB flash drive safely from the computer, do the following:

```
# umount /dev/sdb1
# swapoff /dev/sdb2
# umount /mnt/test
# lvremove /dev/mapper/abc-data
# vgremove abc
# pvremove /dev/sdb3
```

You can now safely remove the USB flash drive from the computer.

Chapter 13: Understanding Server Administration

1. To log in to any account on another computer using the ssh command, enter the following and then enter the password when prompted:

```
$ ssh joe@localhost
joe@localhost's password:
*********
[joe]$
```

2. To display the contents of a remote /etc/system-release file and have its contents displayed on the local system using remote execution with the ssh command, do the following:

```
$ ssh joe@localhost "cat /etc/system-release"
joe@localhost's password: *******
Fedora release 30 (Thirty)
```

3. To use X11 forwarding to display a gedit window on your local system and then save a file on the remote home directory, do the following:

```
        $ ssh -X joe@localhost "gedit newfile"
        joe@localhost's password: ********
        $ ssh joe@localhost "cat newfile"
        joe@localhost's password: ********
        This is text from the file I saved in joe's remote home
directory
```

4. To copy all of the files from the /usr/share/selinux directory recursively on a remote system to the /tmp directory on your local system in such a way that all of the modification times on the files are updated to the time on the local system when they are copied, do the following:

```
$ scp -r joe@localhost:/usr/share/selinux /tmp
joe@localhost's password:
 ********
irc.pp.bz2                          100% 9673     9.5KB/s   00:00
dcc.pp.bz2                          100%   15KB  15.2KB/s   00:01
$ ls -l /tmp/selinux | head
total 20
drwxr-xr-x. 3 root root  4096 Apr 18 05:52 devel
drwxr-xr-x. 2 root root  4096 Apr 18 05:52 packages
drwxr-xr-x. 2 root root 12288 Apr 18 05:52 targeted
```

5. To copy all of the files from the /usr/share/logwatch directory recursively on a remote system to the /tmp directory on your local system in such a way that all of the modification times on the files from the remote system are maintained on the local system, try the following:

```
$ rsync -av joe@localhost:/usr/share/logwatch /tmp
joe@localhost's password: ********
```

```
        receiving incremental file list
        logwatch/
        logwatch/default.conf/
        logwatch/default.conf/logwatch.conf
        $ ls -l /tmp/logwatch | head
        total 16
        drwxr-xr-x. 5 root root 4096 Apr 19  2011 default.conf
        drwxr-xr-x. 4 root root 4096 Feb 28  2011 dist.conf
        drwxr-xr-x. 2 root root 4096 Apr 19  2011 lib
```

6. To create a public/private key pair to use for SSH communications (no passphrase on the key), copy the public key file to a remote user's account with ssh-copy-id, and use key-based authentication to log in to that user account without having to enter a password, use the following code:

```
        $ ssh-keygen
        Generating public/private rsa key pair.
        Enter file in which to save the key (/home/joe/.ssh/id_
rsa): ENTER
        /home/joe/.ssh/id_rsa already exists.
        Enter passphrase (empty for no passphrase):  ENTER
        Enter same passphrase again:  ENTER
        Your identification has been saved in /home/joe/.ssh/id_
rsa.
        Your public key has been saved in /home/joe/.ssh/id_rsa.
pub.
        The key fingerprint is:
        58:ab:c1:95:b6:10:7a:aa:7c:c5:ab:bd:f3:4f:89:1e joe@cnegus.
csb
        The key's randomart image is:
        ...
        $ ssh-copy-id -i ~/.ssh/id_rsa.pub joe@localhost
        joe@localhost's password: ********
        Now try logging into the machine, with "ssh 'joe@
localhost'",
        and check in:
        .ssh/authorized_keys
        to make sure we haven't added extra keys that you weren't
expecting.
        $ ssh joe@localhost
        $ cat .ssh/authorized_keys
        ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyN2Psp5/
LRUC9E8BDCx53yPUa0qoOPd

v6H4sF3vmn04V6E7D1iXpzwPzdo4rpvmR1ZiinHR2xGAEr2uZag7feKgLnww2KPcQ6S
        iR7lzrOhQjV+SGb/a1dxrIeZqKMq1Tk07G4EvboIrq//9J47vI4l7iNu0x
RmjI3TTxa
        DdCTbpG6J3uSJm1BKzdUtwb413x35W2bRgMI75aIdeBsDgQBBiOdu+zuTM
rXJj2viCA
```

```
        XeJ7gIwRvBaMQdOSvSdlkX353tmIjmJheWdgCccM/1jKdoELpaevg9anCe/
yUP3so31
        tTo4I+qTfzAQD5+66oqW0LgMkWVvfZI7dUz3WUPmcMw== chris@abc.
example.com
```

7. To create an entry in /etc/rsyslog.conf that stores all authentication messages at the info level and higher into a file named /var/log/myauth, do the following. Watch from one terminal as the data comes in.

```
        # vim /etc/rsyslog.conf
        authpriv.info                                /var/log/myauth
        # service rsyslog restart
             or
        # systemctl restart rsyslog.service
        <Terminal 1>                                <Terminal 2>
        # tail -f /var/log/myauth                   $ ssh joe@
localhost
        Apr 18 06:19:34 abc unix_chkpwd[30631]   joe@localhost's
password:
        Apr 18 06:19:34 abc sshd[30631]          Permission
denied,try again
         :pam_unix(sshd:auth):
         authentication failure;logname= uid=501
         euid=501 tty=ssh ruser= rhost=localhost
         user=joe
        Apr 18 06:19:34 abc sshd[30631]:
         Failed password for joe from
         127.0.0.1 port 5564 ssh2
```

8. To determine the largest directory structures under /usr/share, sort them from largest to smallest, and list the top 10 of those directories in terms of size using the du command, enter the following:

```
        $ du -s /usr/share/* | sort -rn | head
        527800 /usr/share/locale
        277108 /usr/share/fonts
        196232 /usr/share/help

        134984 /usr/share/backgrounds
        ...
```

9. To show the space that is used and available from all of the filesystems currently attached to the local system, but exclude any tmpfs or devtmpfs filesystems by using the df command, enter the following:

```
        $ df -h -x tmpfs -x devtmpfs
        Filesystem      Size  Used Avail Use% Mounted on
        /deev/sda4       20G  4.2G 16G    22% /
```

10. To find any files in the /usr directory that are more than 10MB in size, do the following:

```
        $ find /usr -size +10M
        /usr/lib/locale/locale-archive
        /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.212.b04-0.fc30.
x86_64/jre/lib/rt.jar
        /usr/libexec/cni/dhcp
        /usr/libexec/gdb
        /usr/libexec/gcc/x86_64-redhat-linux/9/lto1
        /usr/libexec/gcc/x86_64-redhat-linux/9/cc1
```

Chapter 14: Administering Networking

1. To use the desktop to check that NetworkManager has successfully started your network interface (wired or wireless), do the following:
   a. Left-click the upper-right corner of your GNOME desktop to see the drop-down menu. Any active wired or wireless network connections should appear on that menu.
   b. If it has not connected to the network, select from the list of wired or wireless networks available, and then enter the username and password, if prompted, to start an active connection.
2. To run a command to check the active network interfaces available on your computer, enter the following:

```
        $ ifconfig
```

or

```
        $ ip addr show
```

3. Try to contact google.com from the command line in a way that ensures that DNS is working properly:

```
        $ ping google.com
        Ctrl-C
```

4. To run a command to check the routes being used to communicate outside of your local network, enter the following:

```
        $ route
```

5. To trace the route being taken to connect to google.com, use the traceroute command:

```
        $ traceroute google.com
```

6. To view the network interfaces and related network activities for your Linux system through Cockpit, open a web browser to port 9090 using an IP address or hostname. For example: https://localhost:9090/network.

7. To create a host entry that allows you to communicate with your local host system using the name myownhost, edit the /etc/hosts file (vi /etc/hosts), and add myownhost to the end of the localhost entry so that it appears as follows (then ping myownhost to see if it worked):

```
127.0.0.1        localhost.localdomain localhost myownhost
# ping myownhost
Ctrl+C
```

8. To see the DNS name servers being used to resolve hostnames and IP addresses on your system (yours will be different than those shown below), enter the following:

```
# cat /etc/resolv.conf
        nameserver 10.83.14.9
        nameserver 10.18.2.10
        nameserver 192.168.1.254
        # dig google.com
        ...
        google.com.     91941   IN     NS     ns3.google.com.
        ;; Query time: 0 msec
        ;; SERVER: 10.18.2.9#53(10.18.2.9)
        ;; WHEN: Sat Nov 23 20:18:56 EST 2019
        ;; MSG SIZE  rcvd: 276
```

9. To create a custom route that directs traffic destined for the 192.168.99.0/255.255.255.0 network to some IP address on your local network, such as 192.168.0.5 (first ensuring that the 192.168.99 network is not being used at your location), do the following:

   a. Determine the name of your network interface, for example enp4s0. In that case, as root run the following commands:

   ```
   # cd /etc/sysconfig/network-scripts
   # vi route-enp4s0
   ```

   b. Add the following lines to that file:

   ```
   ADDRESS0=192.168.99.0
   NETMASK0=255.255.255.0
   GATEWAY0=192.168.0.5
   ```

   c. Restart networking and run route to see that the route is active:

   ```
           # systemctl restart NetworkManager
           # route -n
           Kernel IP routing table
           Destination   Gateway       Genmask        Flags Metric
   Ref Use Iface
           192.168.0.1   0.0.0.0       255.255.255.0  U     600
   0     0 enp4s0
   ```

```
        192.168.99.0  192.168.0.5   255.255.255.0  UG    600
0     0 enp4s0
```

10. To check to see if your system has been configured to allow IPv4 packets to be routed between network interfaces on your system, enter the following:

    ```
    # cat /proc/sys/net/ipv4/ip_forward
    0
    ```

    A `0` shows that IPv4 packet forwarding is disabled; a `1` shows that it is enabled.

Chapter 15: Starting and Stopping Services

1. To determine which initialization daemon your server is currently using, consider the following:

   a. In most cases today, PID 1 appears as the `systemd` daemon:

   ```
           # ps -ef | head
           UID        PID  PPID  C STIME TTY          TIME CMD
           root         1     0  0 17:01 ?        00:00:04 /usr/
   lib/systemd/systemd --
                switched-root --system --deserialize 18
   ```

   If you type `ps -ef` and PID 1 is `init`, it still might be the `systemd` daemon. Use the `strings` command to see if `systemd` is in use:

   ```
   # strings /sbin/init | grep -i systemd
   systemd.unit=
   systemd.log_target=
   systemd.log_level=
   ...
   ```

   b. Most likely, you have the Upstart, SysVinit, or BSD `init` daemon if your `init` daemon is not `systemd`. But double-check at `http://wikipedia.org/wiki/Init`.

2. The tools you use to manage services depend primarily on which initialization system is in use. Try to run the `systemctl` and `service` commands to determine the type of initialization script in use for the `ssh` service on your system:

   a. For `systemd`, a positive result, shown here, means that the `sshd` has been converted to `systemd`:

   ```
           # systemctl status sshd.service
           sshd.service - OpenSSH server daemon
             Loaded: loaded (/lib/systemd/system/sshd.service;
   enabled)
             Active: active (running) since Mon, 20 Apr 2020
   12:35:20...
   ```

   b. If you don't see positive results for the preceding test, try the following command for the SysVinit `init` daemon. A positive result here, along with negative results for the preceding tests, means that sshd is still using the SysVinit daemon.

```
# service ssh status
sshd (pid 2390) is running...
```

3. To determine your server' previous and current runlevel, use the runlevel command. It still works on all init daemons:

```
$ runlevel
N 3
```

4. To change the default runlevel or target unit on your Linux server, you can do one of the following (depending upon your server's init daemon):

   a. For SysVinit, edit the file /etc/inittab and change the # in the line id:#:initdefault: to 2, 3, 4, or 5.

   b. For systemd, change the default.target to the desired runlevel#.target, where # is 2, 3, 4, or 5. The following shows you how to change the target unit to runlevel3.target.

```
# systemctl set-default runlevel3.target
Removed /etc/systemd/system/default.target.
Created symlink /etc/systemd/system/default.target →
   /usr/lib/systemd/system/multi-user.target.
```

5. To list out services running (or active) on your server, you need to use different commands, depending upon the initialization daemon you are using.

   a. For SysVinit, use the service command as shown in this example:

```
# service --status-all | grep running | sort
anacron (pid 2162) is running...
atd (pid 2172) is running...
```

   b. For systemd, use the systemctl command, as follows:

```
# systemctl list-unit-files --type=service | grep -v disabled
UNIT FILE                                       STATE
abrt-ccpp.service                               enabled
abrt-oops.service                               enabled
...
```

6. To list out the running (or active) services on your Linux server, use the appropriate command(s) determined in answer 5 for the initialization daemon that your server is using.

7. For each initialization daemon, the following command(s) show a particular service's current status:

   a. For SysVinit, the service *service_name* status command is used.

   b. For systemd, the systemctl status *service_name* command is used.

8. To show the status of the cups daemon on your Linux server, use the following:

   a. For the SysVinit:

   ```
   # service cups status
   cupsd (pid 8236) is running...
   ```

   b. For systemd:

   ```
   # systemctl status cups.service
   cups.service - CUPS Printing Service
   Loaded: loaded (/lib/systemd/system/cups.service; enabled)
   Active: active (running) since Tue, 05 May 2020 04:43:5...
   Main PID: 17003 (cupsd)
   CGroup: name=systemd:/system/cups.service
   17003 /usr/sbin/cupsd -f
   ```

9. To attempt to restart the cups daemon on your Linux server, use the following:

   a. For SysVinit:

   ```
   # service cups restart
   Stopping cups:          [  OK  ]
   ```

   b. For systemd:

   ```
   # systemctl restart cups.service
   ```

10. To attempt to reload the cups daemon on your Linux server, use the following:

    a. For SysVinit:

    ```
    # service cups reload
    Reloading cups: [ OK ]
    ```

    b. For systemd, this is a trick question. You cannot reload the cups daemon on a systemd Linux server!

    ```
    # systemctl reload cups.service
    Failed to issue method call: Job type reload is
      not applicable for unit cups.service.
    ```

Chapter 16: Configuring a Print Server

For questions that involve working with printers, you can use either graphical or command-line tools in most cases. The point is to make sure that you get the correct results, shown in the answers that follow. The answers here include a mix of graphical and command-line ways of solving the exercises. (Become root user when you see a # prompt.)

1. To use the Print Settings window to add a new printer called myprinter to your system (generic PostScript printer, connected to a port), do the following from Fedora 30:

   a. Install the system-config-printer package:

   ```
   # dnf install system-config-printer
   ```

   b. From the GNOME 3 desktop, select Print Settings from the Activities screen.

   c. Unlock the interface and enter the root password.

   d. Select the Add button.

   e. Select a USB or other port as the device and click Forward.

   f. For the driver, choose Generic and click Forward; then choose PostScript and click Forward.

   g. Click Forward to skip any installable options, if needed.

   h. For the printer name, call it `myprinter`, give it any description and location you like, and click Apply.

   i. Click Cancel in order not to print a test page. The printer should appear in the Print Settings window.

2. To use the `lpstat -t` command to see the status of all of your printers, enter the following:

```
        # lpstat -t
        deskjet-5550 accepting requests since Mon 02 Mar 2020
07:30:03 PM EST
```

3. To use the `lpr` command to print the `/etc/hosts` file, enter the following:

```
        $ lp /etc/hosts -P myprinter
```

4. To check the print queue for that printer, enter the following:

```
        # lpq -P myprinter
        myprinter is not ready
        Rank    Owner   Job     File(s)             Total Size
        1st     root    655     hosts               1024 bytes
```

5. To remove the print job from the queue (cancel it), enter the following.

```
        # lprm -P myprinter
```

6. To use the printing window to set the basic server setting that publishes your printers so that other systems on your local network can print to your printers, do the following:

   a. On a GNOME 3 desktop, from the Activities screen, type **Print Settings** and press Enter.

   b. Select Server ➪ Settings and type the root password if prompted.

   c. Click the check box next to “Publish shared printers connected to this system” and click OK.

7. To allow remote administration of your system from a web browser, follow these steps:
   a. On a GNOME 3 desktop, from the Activities screen, type **Print Settings**, and press Enter.
   b. Select Server ➪ Settings and type the root password if prompted.
   c. Click the check box next to "Allow remote administration" and click OK.
8. To demonstrate that you can do remote administration of your system from a web browser on another system, do the following:
   a. In the location box from a browser window from another computer on your network, enter the following, replacing ***hostname*** with the name or IP address of the system running your print service: **http://*hostname*:631**.
   b. Type **root** as the user and the root password, when prompted. The CUPS home page should appear from that system.
9. To use the netstat command to see on which addresses the cupsd daemon is listening, enter the following:

```
# netstat -tupln | grep 631
tcp    0    0 0.0.0.0:631      0.0.0.0:*      LISTEN    6492/cupsd
tcp6   0    0 :::631           :::*           LISTEN    6492/cupsd
```

10. To delete the myprinter printer entry from your system, do the following:
    a. Click the Unlock button and type the root password when prompted.
    b. From the Print Settings window, right-click the myprinter icon and select Delete.
    c. When prompted, select Delete again.

Chapter 17: Configuring a Web Server

1. To install all of the packages associated with the Web Server group on a Fedora system, do the following:

```
# yum groupinstall "Web Server"
```

2. To create a file called index.html in the directory assigned to DocumentRoot in the main Apache configuration file (with the words "My Own Web Server" inside), do the following:
   a. Determine the location of DocumentRoot:

```
# grep ^DocumentRoot /etc/httpd/conf/httpd.conf

DocumentRoot "/var/www/html"
```

b. Echo the words "My Own Web Server" into the index.html file located in DocumentRoot:

```
# echo "My Own Web Server" > /var/www/html/index.html
```

3. To start the Apache web server and set it to start up automatically at boot time, then check that it is available from a web browser on your local host, do the following. (You should see the words "My Own Web Server" displayed if it is working properly.)

   The httpd service is started and enabled differently on different Linux systems. In recent Fedora 30 or RHEL 7 or 8, enter the following:

```
# systemctl start httpd.service
# systemctl enable httpd.service
```

   In RHEL 6 or earlier, enter the following:

```
# service httpd start
# chkconfig httpd on
```

4. To use the netstat command to see on which ports the httpd server is listening, enter the following:

```
# netstat -tupln | grep httpd
tcp6     0   0 :::80      :::*    LISTEN   2496/httpd
tcp6     0   0 :::443     :::*    LISTEN   2496/httpd
```

5. Try to connect to your Apache web server from a web browser that is outside of the local system. If it fails, correct any problems that you encounter by investigating the firewall, SELinux, and other security features.

   If you don't have DNS set up yet, use the IP address of the server to view your Apache server from a remote web browser, such as http://192.168.0.1. If you are not able to connect, retry connecting to the server from your browser after performing each of the following steps on the system running the Apache server:

```
# iptables -F
# setenforce 0
# chmod 644 /var/www/html/index.html
```

   The iptables -F command flushes the firewall rules temporarily. If connecting to the web server succeeds after that, you need to add new firewall rules to open tcp ports 80 and 443 on the server. On a system using the firewalld service, do this by clicking the check box next to those ports on the Firewall window. For systems running the iptables service, add the following rules before the last DROP or REJECT rule.

```
        -A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j
ACCEPT
        -A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j
ACCEPT
```

The `setenforce 0` command puts SELinux in permissive mode temporarily. If connecting to the web server succeeds after that, you need to correct SELinux file context and/or Boolean issues (probably file context in this case). The following should work:

```
# chcon --reference=/var/www/html /var/www/html/index.html
```

If the `chmod` command works, it means that the Apache user and group did not have read permission to the file. You should be able to leave the new permissions as they are.

6. To use the `openssl` or similar command to create your own private RSA key and self-signed SSL certificate, do the following:

```
# yum install openssl
# cd /etc/pki/tls/private
# openssl genrsa -out server.key 1024
# chmod 600 server.key
# cd /etc/pki/tls/certs
# openssl req -new -x509 -nodes -sha1 -days 365 \
   -key /etc/pki/tls/private/server.key \
   -out server.crt
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: NJ
Locality Name (eg, city) []: Princeton
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:TEST USE ONLY
Organizational Unit Name (eg, section) []:TEST USE ONLY
Common Name (eg, YOUR name) []:secure.example.org
Email Address []:dom@example.org
```

   You should now have a `/etc/pki/tls/private/server.key` key file and a `/etc/pki/tls/certs/server.crt` certificate file.

7. To configure your Apache web server to use your key and self-signed certificate to serve secure (HTTPS) content, do the following:

   a. Edit the `/etc/httpd/conf.d/ssl.conf` file to change the key and certificate locations to use the ones that you just created:

```
SSLCertificateFile /etc/pki/tls/certs/server.crt
SSLCertificateKeyFile /etc/pki/tls/private/server.key
```

   b. Restart the httpd service:

```
# systemctl restart httpd.service
```

8. To use a web browser to create an HTTPS connection to your web server and view the contents of the certificate that you created, do the following:

From the system running the Apache server, type **https://localhost** in the browser's location box. You should see a message that reads, "This Connection is Untrusted." To complete the connection, do the following:

a. Click I Understand the Risks.

b. Click Add Exception.

c. Click Get Certificate.

d. Click Confirm Security Exception.

9. To create a file named /etc/httpd/conf.d/example.org.conf, which turns on name-based virtual hosting and creates a virtual host that (1) listens on port 80 on all interfaces, (2) has a server administrator of joe@example.org, (3) has a server name of joe.example.org, (4) has a DocumentRoot of /var/www/html/joe.example.org, and (5) has a DirectoryIndex that includes at least index.html and then create an index.html file in DocumentRoot that contains the words "Welcome to the House of Joe" inside, do the following.

Create an example.org.conf file that looks like the following:

```
NameVirtualHost *:80
<VirtualHost *:80>
    ServerAdmin     joe@
example.org
    ServerName      joe.
example.org
    ServerAlias     web.example.org
    DocumentRoot    /var/www/html/joe.example.org/
    DirectoryIndex  index.html
</VirtualHost>
```

This is how you could create the text to go into the index.html file:

```
# echo "Welcome to the House of Joe" > \
     /var/www/html/joe.example.org/index.html
```

10. To add the text joe.example.org to the end of the localhost entry in your /etc/hosts file on the machine that is running the web server, and check it by typing **http://joe.example.org** into the location box of your web browser to see "Welcome to the House of Joe" when the page is displayed, do the following:

a. Reload the httpd.conf file modified in the previous exercise in one of two ways:

```
# apachectl graceful
# systemctl restart httpd
```

b. Edit the /etc/hosts file with any text editor, so the local host line appears as follows:

```
        127.0.0.1      localhost.localdomain localhost joe.
example.org
```

c. From a browser on the local system where httpd is running, you should be able to type **http://joe.example.org** into the location box to access the Apache web server using name-based authentication.

Chapter 18: Configuring an FTP Server

Caution

Don't do the tasks described here on a working, public FTP server, because these tasks will interfere with its operations. (You could, however, use these tasks to set up a new FTP server.)

1. To determine which package provides the Very Secure FTP Daemon service, enter the following as root:

   ```
   # yum search "Very Secure FTP"
   ...
   ================ N/S Matched: Very Secure FTP ============
   vsftpd.i686 : Very Secure Ftp Daemon
   ```

   The search found the vsftpd package.

2. To install the Very Secure FTP Daemon package on your system and search for the configuration files in the vsftpd package, enter the following:

   ```
   # yum install vsftpd
   # rpm -qc vsftpd | less
   ```

3. To enable anonymous FTP and disable local user login for the Very Secure FTP Daemon service, set the following in the /etc/vsftpd/vsftpd.conf file:

   ```
   anonymous_enable=YES
   write_enable=YES
   anon_upload_enable=YES
   local_enable=NO
   ```

4. To start the Very Secure FTP Daemon service and set it to start when the system boots, enter the following on a current Fedora or Red Hat Enterprise Linux system:

   ```
   # systemctl start vsftpd.service
   # systemctl enable vsftpd.service
   ```

On a Red Hat Enterprise Linux 6 system, enter the following:

```
# service vsftpd start
# chkconfig vsftpd on
```

5. On the system running your FTP server, enter the following to create a file named `test` in the anonymous FTP directory that contains the words "Welcome to your vsftpd server":

   ```
   # echo "Welcome to your vsftpd server" > /var/ftp/test
   ```

6. To open the `test` file from the anonymous FTP home directory using a web browser on the system running your FTP server, do the following.

   Open a web browser, enter the following in the location box, and press Enter:

   ```
   ftp://localhost/test
   ```

   The text "Welcome to your vsftpd server" should appear in the browser window.

7. To access the `test` file in the anonymous FTP home directory, do the following. (If you cannot access the file, check that your firewall, SELinux, and TCP wrappers are configured to allow access to that file, as described here.)

   a. Enter the following into the location box of a browser on a system on your network that can reach the FTP server (replace *`host`* with your system's fully qualified hostname or IP address):

      ```
      ftp://host/test
      ```

      If you cannot see the welcome message in your browser window, check what may be preventing access. To turn off your firewall temporarily (flush your `iptables` rules), enter the following command as the root user from a shell on your FTP server system and then try to access the site again:

      ```
      # iptables -F
      ```

   b. To disable SELinux temporarily, enter the following and then try to access the site again:

      ```
      # setenforce 0
      ```

   After you have determined what is causing the file on your FTP server to be unavailable, go back to the section "Securing Your FTP Server" in Chapter 18, and go through the steps to determine what might be blocking access to your file. These are the likely possibilities:

   c. For `iptables`, make sure that there is a rule opening TCP port 21 on the server.

   d. For SELinux, make sure that the file context is set to `public_content_t`.

8. To configure your vsftpd server to allow file uploads by anonymous users to a directory named `in`, do the following as root on your FTP server:

   a. Create the `in` directory as follows:

   ```
   # mkdir /var/ftp/in
   # chown ftp:ftp /var/ftp/in
   # chmod 777 /var/ftp/in
   ```

   b. For a recent Fedora or RHEL, open the Firewall Configuration window and check the FTP box under services to open access to your FTP service. For earlier RHEL and Fedora systems, configure your `iptables` firewall to allow new requests on TCP port 21 by adding the following rule at some point before a final `DROP` or `REJECT` rule in your `/etc/sysconfig/iptables` file:

   ```
           -A INPUT -m state --state NEW -m tcp -p tcp --dport 21
   -j ACCEPT
   ```

   c. Configure your `iptables` firewall to do connection tracking by loading the appropriate module to the `/etc/sysconfig/iptables-config` file:

   ```
   IPTABLES_MODULES="nf_conntrack_ftp"
   ```

   d. For SELinux to allow uploading to the directory, first set file contexts properly:

   ```
           # semanage fcontext -a -t public_content_rw_t "/var/ftp/
   in(/.*)?"
           # restorecon -F -R -v /var/ftp/in
   ```

   e. Next, set the SELinux Boolean to allow uploading:

   ```
   # setsebool -P allow_ftpd_anon_write on
   ```

   f. Restart the `vsftpd` service (`service vsftpd restart` or `systemctl restart vsftpd.service`).

9. To install the `lftp` FTP client (if you don't have a second Linux system, install `lftp` on the same host running the FTP server). Optionally, try to upload the `/etc/hosts` file to the `in` directory on the server, to make sure it is accessible. Run the following commands as the root user:

   ```
   # yum install lftp
   # lftp localhost
   lftp localhost:/> cd in
   lftp localhost:/in> put /etc/hosts
   89 bytes transferred
   lftp localhost:/in> quit
   ```

   You won't be able to see that you copied the `hosts` file to the incoming directory. However, enter the following from a shell on the host running the FTP server to make sure that the `hosts` file is there:

   ```
   # ls /var/ftp/in/hosts
   ```

If you cannot upload the file, troubleshoot the problem as described in Exercise 7, recheck your vsftpd.conf settings, and review the ownership and permissions on the /var/ftp/in directory.

10. Using any FTP client you choose, visit the /pub/debian-meetings directory on the ftp://ftp.gnome.org site and list the contents of that directory. Here's how to do that with the lftp client:

```
# lftp ftp://ftp.gnome.org/pub/debian-meetings/
cd ok, cwd=/pub/debian-meetings
lftp ftp.gnome.org:/pub/debian-meetings>> ls
drwxr-xr-x    3 ftp      ftp            3 Jan 13  2014 2004
drwxr-xr-x    6 ftp      ftp            6 Jan 13  2014 2005
drwxr-xr-x    8 ftp      ftp            8 Dec 20  2006 2006
...
```

Chapter 19: Configuring a Windows File Sharing (Samba) Server

1. To install the samba and samba-client packages, enter the following as root from a shell on the local system:

```
# yum install samba samba-client
```

2. To start and enable the smb and nmb services, enter the following as root from a shell on the local system:

```
# systemctl enable smb.service
# systemctl start smb.service
# systemctl enable nmb.service
# systemctl start nmb.service
```

or

```
# chkconfig smb on
# service smb start
# chkconfig nmb on
# service nmb start
```

3. To set the Samba server's workgroup to TESTGROUP, the NetBIOS name to MYTEST, and the server string to Samba Test System, as root user in a text editor, open the /etc/samba/smb.conf file, and change three lines so that they appear as follows:

```
workgroup = TESTGROUP
netbios name = MYTEST
server string = Samba Test System
```

4. To add a Linux user named phil to your system, and add a Linux password and Samba password for phil, enter the following as root user from a shell. (Be sure to remember the passwords you set.)

```
# useradd phil
# passwd phil
New password: *******
Retype new password: *******
# smbpasswd -a phil
New SMB password: *******
Retype new SMB password: *******
Added user phil.
```

5. To set the [homes] section so that home directories are browseable (yes) and writeable (yes), and that phil is the only valid user, open the /etc/samba/smb.conf file as root, and change the [homes] section so that it appears as follows:

```
[homes]
        comment = Home Directories
        browseable = Yes
        read only = No
        valid users = phil
```

6. To set SELinux Booleans that are necessary to make it so that phil can access his home directory via a Samba client, enter the following as root from a shell, and restart the smb and nmb services:

```
# setsebool -P samba_enable_home_dirs on
# systemctl restart smb
# systemctl restart nmb
```

7. From the local system, use the smbclient command to list that the homes share is available.

```
# smbclient -L localhost
Enter TESTGROUP\root's password: <ENTER>
Anonymous login successful

     Sharename       Type      Comment
     ---------       ----      -------
     homes           Disk      Home Directories
  ...
```

8. To connect to the homes share from a Nautilus (file manager) window on the Samba server's local system for the user phil in a way that allows you to drag and drop files to that folder, do the following:

   a. Open the Nautilus window (select the files icon).

   b. In the left pane, select Other Locations and then click in the Connect to Server box.

   c. Type the Server address. For example, smb://localhost/phil/.

d. When prompted, select Registered User, type **phil** as the username, enter the domain (TESTGROUP), and enter phil's password.

e. Open another Nautilus window and drop a file to phil's homes folder.

9. To open up the firewall so that anyone who has access to the server can access the Samba service (smbd and nmbd daemons), you can simply open the Firewall Configuration window and check the samba and samba-client check boxes (for both Runtime and Permanent). If your system is running basic iptables (and not the firewalld service), change the /etc/sysconfig/iptables file so that the firewall appears like the following (the rules you add being those in bold):

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-I INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-I INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-I INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
-I INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Then enter the following for the firewall rules to be reloaded:

```
# service iptables restart
```

10. To open the homes share again as the user phil from another system on your network (Windows or Linux), and make sure that you can drag and drop fles to it, do the following:

a. This step is really just repeating the Nautilus example described previously or accessing a Windows File Explorer window and opening the share (by selecting Network, then the Samba server). The trick is to make sure that the service has been made available through the Linux server security features.

b. If you cannot access the Samba share, try disabling your firewall and then disabling SELinux. If the share is accessible when you turn off either of those services, go back and debug the problems with the service that is not working:

```
# setenforce 0
# service iptables stop
```

c. When you have fixed the problem, set SELinux back to Enforcing mode and restart iptables:

```
# setenforce 1
# service iptables start
```

Chapter 20: Configuring an NFS File Server

1. To install the packages needed to configure the NFS service on your chosen Linux system, enter the following as root user at a shell (Fedora or RHEL):

```
# yum install nfs-utils
```

2. To list the documentation files that come in the package that provides the NFS server software, enter the following:

```
# rpm -qd nfs-utils
/usr/share/doc/nfs-utils-1.2.5/ChangeLog
...
/usr/share/man/man5/exports.5.gz
/usr/share/man/man5/nfs.5.gz
/usr/share/man/man5/nfsmount.conf.5.gz
/usr/share/man/man7/nfsd.7.gz
/usr/share/man/man8/blkmapd.8.gz
/usr/share/man/man8/exportfs.8.gz
...
```

3. To start and enable the NFS service, enter the following as root user on the NFS server:

```
# systemctl start nfs-server.service
# systemctl enable nfs-server.service
```

4. To check the status of the NFS service that you just started on the NFS server, enter the following as root user:

```
# systemctl status nfs-server.service
```

5. To share a directory /var/mystuff from your NFS server as available to everyone, read-only, and with the root user on the client having root access to the share, first create the mount directory as follows:

```
# mkdir /var/mystuff
```

Then create an entry in the /etc/exports file that is similar to the following:

```
/var/mystuff   *(ro,no_root_squash,insecure)
```

To make the share available, enter the following:

```
# exportfs -v -a
exporting *:/var/mystuff
```

6. To make sure that the share you created is accessible to all hosts, first check that `rpcbind` is not blocked by TCP wrappers by adding the following entry to the beginning of the `/etc/hosts.allow` file:

   ```
   rpcbind: ALL
   ```

   a. To open the firewall in systems that use `firewalld` (RHEL 8 and recent Fedora systems), install the firewall-config package. Then run `firewall-config`. From the Firewall Configuration window that appears, make sure that nfs and rpc-bind are checked to On for the Permanent firewall settings.

   b. To open the ports needed to allow clients to reach NFS through the `iptables` firewall (RHEL 6 and earlier Fedora systems without `firewalld`), you need to open at least TCP and UDP ports 111 (`rpcbind`), 20048 (`mountd`), and 2049 (`nfs`) by adding the following rules to the `/etc/sysconfig/iptables` file and starting the `iptables` service:

   ```
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 111 -j ACCEPT
   -A INPUT -m state --state NEW -m udp -p udp --dport 111 -j ACCEPT
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT
   -A INPUT -m state --state NEW -m udp -p udp --dport 2049 -j ACCEPT
   -A INPUT -m state --state NEW -m tcp -p tcp --dport 20048 -j ACCEPT
   -A INPUT -m state --state NEW -m udp -p udp --dport 20048 -j ACCEPT
   ```

   SELinux should be able to share NFS filesystems while in enforcing mode without any changes to file contexts or Booleans. To make sure that the share you created can be shared read-only, run the following command as root user on the NFS server:

   ```
   # setsebool -P nfs_export_all_ro on
   ```

7. To view the shares available from the NFS server, assuming that the NFS server is named `nfsserver`, enter the following from the NFS client:

   ```
   # showmount -e nfsserver
   Export list for nfsserver:
   /var/mystuff  *
   ```

8. To create a directory called `/var/remote` and temporarily mount the `/var/mystuff` directory from the NFS server (named `nfsserver` in this example) on that mount point, enter the following as root user from the NFS client:

   ```
   # mkdir /var/remote
   # mount -t nfs nfsserver:/var/mystuff /var/remote
   ```

9. To add an entry so that the same mount is done automatically when you reboot, first unmount `/var/remote` as follows:

   ```
   # umount /var/remote
   ```

Then add an entry like the following to the /etc/fstab on the client system:

```
/var/remote   nfsserver:/var/mystuff  nfs bg,ro 0 0
```

To test that the share is configured properly, enter the following on the NFS client as the root user:

```
# mount -a
# mount -t nfs4
nfsserver:/var/mystuff on /var/remote type nfs4
 (ro,vers=4,rsize=524288...
```

10. To copy some files to the /var/mystuff directory, enter the following on the NFS server:

```
# cp /etc/hosts /etc/services /var/mystuff
```

From the NFS client, to make sure that you can see the files just added to that directory, and to make sure that you can't write files to that directory from the client, enter the following:

```
        # ls /var/remote
        hosts    services
        # touch /var/remote/file1
        touch: cannot touch '/var/remote/file1': Read-only file
system
```

Chapter 21: Troubleshooting Linux

1. To go into Setup mode from the BIOS screen on your computer, do the following:
   a. Reboot your computer.
   b. Within a few seconds, you should see the BIOS screen, with an indication of which function key to press to go into Setup mode. (On my Dell workstation, it's the F2 function key.)
   c. The BIOS screen should appear. (If the system starts booting Linux, you didn't press the function key fast enough.)
2. From the BIOS setup screen, do the following to determine whether your computer is 32-bit or 64-bit, whether it includes virtualization support, and whether your network interface card is capable of PXE booting.

   Your experience may be a bit different from mine, depending on your computer and Linux system. The BIOS setup screen is different for different computers. In general, however, you can use arrow keys and tab keys to move between different columns, and press Enter to select an entry.

   a. On my Dell workstation, under the System heading, I highlight Processor Info to see that mine is a 64-bit Technology computer. Look in the Processor Info section, or a similar, section on your computer, to see the type of processor that you have.

   b. On my Dell workstation, under the Onboard Devices heading, I highlight Integrated NIC and press Enter. The Integrated NIC screen that appears to the right lets me choose to enable or disable the NIC (On or Off) or enable with PXE or RPL (if I intend to boot the computer over the network).

3. To interrupt the boot process to get to the GRUB boot loader, do the following:

   a. Reboot the computer.

   b. Just after the BIOS screen disappears, when you see the countdown to booting the Linux system, press any key (perhaps the spacebar).

   c. The GRUB boot loader menu should appear, ready to allow you to select which operating system kernel to boot.

4. To boot up your computer to runlevel 1 so that you can do some system maintenance, get to the GRUB boot screen (as described in the previous exercise), and then do the following:

   a. Use the arrow keys to highlight the operating system and kernel that you want to boot.

   b. Type **e** to see the entries needed to boot the operating system.

   c. Move your cursor to the line that included the kernel. (It should include the word `vmlinuz` somewhere on the line.)

   d. Move the cursor to the end of that line, add a space, and then type **init=bash**.

   e. Follow the instructions to boot the new entry. You will probably either press Ctrl+X or press Enter; if there is another screen, type **b**.

   If it worked, your system should bypass the login prompt and boot up directly to a root user shell where you can do administrative tasks without providing a password.

5. To look at the messages that were produced in the kernel ring buffer (which shows the activity of the kernel as it booted up), enter the following from the shell after the system finishes booting:

```
# dmesg | less
```

6. Or, on a system using `systemd`, enter the following:

```
# journalctl -k
```

7. To run a trial `yum update` from Fedora or RHEL and exclude any kernel package that is available, enter the following (when prompted, type **N** to not actually go through with the update, if updates are available):

   ```
   # yum update --exclude='kernel*'
   ```

8. To check to see what processes are listening for incoming connections on your system, enter the following:

   ```
   # netstat -tupln | less
   ```

9. To check to see what ports are open on your external network interface, do the following.

   If possible, run the `nmap` command from another Linux system on your network, replacing *yourhost* with the hostname or IP address of your system:

   ```
   # nmap yourhost
   ```

10. To clear your system's page cache and watch the effect it has on your memory usage, do the following:

    a. Select Terminal from an application menu on your desktop (it is located on different menus for different systems).

    b. Run the `top` command (to watch processes currently running on your system), and then type a capital **M** to sort processes by those consuming the most memory.

    c. From the Terminal window, select File and Open Terminal to open a second Terminal window.

    d. From the second Terminal window, become root user (`su -`).

    e. While watching the `Mem` line (used column) in the first Terminal window, enter the following from the second Terminal window:

    ```
    # echo 3 > /proc/sys/vm/drop_caches
    ```

    f. The used `RES` memory should go down significantly on the `Mem` line. The numbers in the `RES` column for each process should go down as well.

11. To view memory and swap usage from Cockpit through your web browser, open your browser to Cockpit for your host (`https://hostname:9090`). Then select System ➪ Memory & Swap.

Chapter 22: Understanding Basic Linux Security

1. To check log messages from the `systemd` journal for the `NetworkManager.service`, `sshd.service`, and `auditd.service` services, enter the following:

   ```
   # journalctl -u NetworkManager.service
   ...
   ```

```
# journalctl -u sshd.service
...
# journalctl -u auditd.service
...
```

2. User passwords are stored in the /etc/shadow file. To see its permissions, type **ls -l /etc/shadow** at the command line. (If no shadow file exits, then you need to run pwconv.)

   The following are the appropriate settings:

   ```
    # ls -l /etc/shadow
   ----------. 1 root root 1049 Feb  10 09:45 /etc/shadow
   ```

3. To determine your account's password aging and whether it will expire using a single command, type chage -l *user _ name*. For example:

   ```
   # chage -l chris
   ```

4. To start auditing writes to the /etc/shadow with the auditd daemon, enter the following at the command line:

   ```
   # auditctl -w /etc/shadow -p w
   ```

   To check your audit settings, type in auditctl -l at the command line.

5. To create a report from the auditd daemon on the /etc/shadow file, enter ausearch -f /etc/shadow at the command line. To turn off the auditing on that file, enter auditctl -W /etc/shadow -p w at the command line.

6. To install the lemon package, damage the /usr/bin/lemon file, verify that the file has been tampered with, and remove the lemon package, enter the following:

   ```
   # yum install -y lemon
   # cp /etc/services /usr/bin/lemon
   # rpm -V lemon
   S.5....T.    /usr/bin/lemon
   # yum erase lemon
   ```

   From the original lemon file, the file size (S), the md4sum (5), and the modification times (T) all differ. For Ubuntu, install the package with apt-get install lemon and enter debsums lemon to check it.

7. If you suspect that you have had a malicious attack on your system today and important binary files have been modified, you can find these modified files by entering the following at the command line: find directory -mtime -1 for the directories, /bin, /sbin, /usr/bin, and /usr/sbin.

8. To install and run chkrootkit to see if the malicious attack from the exercise above installed a rootkit, choose your distribution and do the following:

   a. To install on a Fedora or RHEL distribution, enter yum install chkrootkit at the command line.

b. To install on an Ubuntu or Debian-based distribution, enter `sudo apt-get install chkrootkit` at the command line.

c. To run the check, enter `chkrootkit` at the command line and review the results.

9. To find files anywhere in the system with the SUID or SGID permission set, enter `find / -perm /6000 -ls` at the command line.

10. To install the aide package, run the aide command to initialize the aide database, copy the database to the correct location, and run the aide command to check whether any important files on your system have been modified, enter the following.

```
# yum install aide
# aide -i
# cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
# aide -C
```

To make the output more interesting, you could install the lemon package (described in an earlier exercise) before you run `aide -i`, and modify it before running `aide -C` to see how a modified binary looks from aide.

Chapter 23: Understanding Advanced Linux Security

To do the first few exercises, you must have the gnupg2 package installed. This is not installed by default in Ubuntu, although it is installed for the latest Fedora and RHEL releases.

1. To encrypt a file using the gpg2 utility and a symmetric key, enter the following command. (The gpg2 utility asks for a passphrase to protect the symmetric key.)

```
$ gpg2 -c filename
```

2. To generate a key pair using the gpg2 utility, enter the following:

```
$ gpg2 --gen-key
```

You must provide the following information:

a. Your real name and email address

b. A passphrase for the private key

3. To list out the keys you generated, enter the following:

```
$ gpg2 --list-keys
```

4. To encrypt a file and add your digital signature using the gpg2 utility, do the following:

a. You must have first generated a key ring (Exercise 2).

b. After you have generated the key ring, enter

```
    $ gpg2 --output EncryptedSignedFile --sign
FiletoEncryptSign
```

5. From the getfedora.org page, select one of the Fedora distributions to download. When the download is complete, select Verify your Download to see instructions for verifying your image. For example, download the appropriate CHECKSUM file for your image, then enter the following:

```
        $ curl https://getfedora.org/static/fedora.gpg | gpg
--import
        $ gpg --verify-files *-CHECKSUM
        $ sha256sum -c *-CHECKSUM
```

6. To determine if the su command on your Linux system is PAM-aware, enter the following:

```
        $ ldd $(which su) | grep pam
        libpam.so.0 => /lib64/libpam.so.0 (0x00007fca14370000)
        ibpam_misc.so.0 => /lib64/libpam_misc.so.0
(0x00007fca1416c000
```

If the su command on your Linux system is PAM-aware, you should see a PAM library name listed when you issue the ldd command.

7. To determine if the su command has a PAM configuration file, type the following:

```
        $ ls /etc/pam.d/su
        /etc/pam.d/su
```

If the file exists, type the following at the command line to display its contents. The PAM contexts it uses include any of the following: auth, account, password, or session.

```
        $ cat /etc/pam.d/su
```

8. To list out the various PAM modules on your Fedora or RHEL system, enter the following:

```
        $ ls /usr/lib64/security/pam*.so
```

To list out the various PAM modules on your Ubuntu Linux system, enter the following:

```
        # find / -name pam*.so
```

9. To find the PAM "other" configuration file on your system, enter ls /etc/pam.d/other at the command line. An "other" configuration file that enforces Implicit Deny should look similar to the following code:

```
        $ cat /etc/pam.d/other
        #%PAM-1.0
        auth     required       pam_deny.so
        account  required       pam_deny.so
        password required       pam_deny.so
        session  required       pam_deny.so
```

10. To find the PAM limits configuration file, enter the following:

```
        $ ls /etc/security/limits.conf
```

Display the file's contents by entering the following:

```
        $ cat /etc/security/limits.conf
```

Settings in this file to prevent a fork bomb look like the following:

```
@student     hard    nproc          50
@student     -       maxlogins       4
```

Chapter 24: Enhancing Linux Security with SELinux

1. To set your system into the permissive mode for SELinux, enter `setenforce permissive` at the command line. It would also be acceptable to enter `setenforce 0` at the command line.
2. To set your system into the enforcing operating mode for SELinux without changing the SELinux primary configuration file, use caution. It is best not to run this command on your system for an exercise until you are ready for the SELinux to be enforced. Use the following command at the command line: `setenforce enforcing`. It would also be acceptable to enter `setenforce 1` at the command line.
3. To find and view the permanent SELinux policy type (set at boot time), go to the main SELinux configuration file, `/etc/selinux/config`. To view it, enter `cat /etc/selinux/config | grep SELINUX=` at the command line. To be sure how it is currently set, enter the `getenforce` command.
4. To list the `/etc/hosts` file security context and identify the different security context attributes, enter `ls -Z /etc/hosts` at the command line:

```
        $ ls -Z /etc/hosts
        -rw-r--r--. root root system_u:object_r:net_conf_t:s0  /
etc/hosts
```

   a. The file's user context is `system_u`, indicating a system file.
   b. The file's role is `object_r`, indicating an object in the file system (a text file, in this case).
   c. The file's type is `net_conf_t`, because the file is a network configuration file.
   d. The file's sensitivity level is `s0`, indicating the lowest security level. (This number may be listed in a range of numbers from `s0-s3`.)
   e. The file's category level starts with a `c` and ends with a number. It may be listed in a range of numbers, such as `c0-c102`. This is not required except in highly secure environments and is not set here.

5. To create a file called `test.html` and assign its type as `httpd_sys_content_t`, enter the following:

```
        $ touch test.html
        $ chcon -t httpd_sys_content_t test.html
        $ ls -Z test.html
        -rw-rw-r--. chris chris unconfined_u:object_r:httpd_sys_
content_t:s0 test.html
```

6. To list the `crond` process's security context and identify the different security context attributes, enter this at the command line:

```
        $ ps -efZ | grep crond
        system_u:system_r:crond_t:s0-s0:c0.c1023 root 665  1  0
            Sep18 ?   00:00:00 /usr/sbin/crond -n
```

   a. The process's user context is `system_u`, indicating a system process.
   b. The process's role is `system_r`, indicating a system role.
   c. The process's type or domain is `crond_t`.
   d. The process's sensitivity level starts `s0-s0`, indicating that it is not highly sensitive. (It is secure by normal Linux standards, however, because the process is run as the root user.)
   e. The process's category level is `c0.c1023`, with the `c0`, indicating that the category is also not highly secure from an SELinux standpoint.

7. To create an `/etc/test.txt` file, change its file context to `user_tmp_t`, restore it to its proper content (the default context for the `/etc` directory), and remove the file, enter the following:

```
        # touch /etc/test.txt
        # ls -Z /etc/test.txt
        -rw-r--r--. root root unconfined_u:object_r:etc_t:s0   /etc/
test.txt
        # chcon -t user_tmp_t /etc/test.txt
        # ls -Z /etc/test.txt
        -rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /
etc/test.txt
        # restorecon /etc/test.txt
        # ls -Z /etc/test.txt
        -rw-r--r--. root root unconfined_u:object_r:etc_t:s0   /etc/
test.txt
        # rm /etc/test.txt
        rm: remove regular empty file `/etc/test.txt'? y
```

8. To determine what Booleans allow anonymous writes and access to the `tftp` service's home directory, then turn those Booleans on permanently, enter the following commands:

```
        # getsebool -a | grep tftp
        tftp_home_dir --> off
        tftpd_anon_write --> off
```

```
...
# setsebool -P tftp_home_dir=on
# setsebool -P tftp_anon_write=on
# getsebool tftp_home_dir tftp_anon_write
tftp_home_dir --> on
tftp_anon_write --> on
```

9. To list all SELinux policy modules on your system, along with their version numbers, enter **semodule –l**.

NOTE

If you wrote `ls /etc/selinux/targeted/modules/active/modules/*.pp` as your answer, that is okay, but this command doesn't give you the version numbers of the policy modules. Only `semodule -l` gives the version numbers.

10. To tell SELinux to allow access to the `sshd` service through TCP Port 54903, enter the following:

```
# semanage port -a -t ssh_port_t -p tcp 54903
# semanage port -l | grep ssh
ssh_port_t                 tcp              54903, 22
```

Chapter 25: Securing Linux on a Network

1. To install the Network Mapper (aka `nmap`) utility on your local Linux system:
   a. On Fedora or RHEL, enter `yum install nmap` at the command line.
   b. On Ubuntu, `nmap` may come pre-installed. If not, enter `sudo apt-get install nmap` at the command line.
2. To run a TCP Connect scan on your local loopback address, enter `nmap -sT 127.0.0.1` at the command line. The ports you have running on your Linux server will vary. However, they may look similar to the following:

```
# nmap -sT 127.0.0.1
        ...
        PORT    STATE SERVICE
        25/tcp  open  smtp
        631/tcp open  ipp
```

3. To run a UDP Connect scan on your Linux system from a remote system:
   a. Determine your Linux server's IP address by entering **ifconfig** at the command line. The output will look similar to the following, and your system's IP address follows `inet addr:` in the `ifconfig` command's output.

```
# ifconfig
...
p2p1  Link encap:Ethernet  HWaddr 08:00:27:E5:89:5A
      inet addr:10.140.67.23
```

   b. From a remote Linux system, enter the command `nmap -sU IP address` at the command line, using the *`IP address`* you obtained from above. For example:

      ```
      # nmap -sU 10.140.67.23
      ```

4. To check to see if your system is running the `firewalld` service, and then install and start it if it is not:
   a. Enter `systemctl status firewalld.service.`
   b. If the `firewalld` service is not running, on a Fedora or RHEL system, enter the following:

      ```
      # yum install firewalld firewall-config -y
      # systemctl start firewalld
      # systemctl enable firewalld
      ```

5. To open ports in your firewall to allow remote access to your local web service, do the following:
   a. Start the Firewall Configuration window (`firewalld-config`).
   b. Make sure that Configuration: Runtime is selected.
   c. Select your current zone (for example, FedoraWorkstation).
   d. Under Services, select the http and https check boxes.
   e. Select Configuration: Permanent.
   f. Under Services, select the http and https check boxes.
6. To determine your Linux system's current `netfilter/iptables` firewall policies and rules, enter `iptables -vnL` at the command line.
7. To save, flush, and restore your Linux system's current firewall rules:
   a. To save your current rules:

      ```
      # iptables-save >/tmp/myiptables
      ```

   b. To flush your current rules:

      ```
      # iptables -F
      ```

   c. To restore the firewall's rules, enter:

      ```
      # iptables-restore < /tmp/myiptables
      ```

8. To set your Linux system's firewall filter table for the input chain to a policy of `DROP`, enter `iptables -P INPUT DROP` at the command line.
9. To change your Linux system firewall's filter table policy back to `accept` for the input chain, enter the following:

   ```
   # iptables -P INPUT ACCEPT
   ```

To add a rule to drop all network packets from the IP address 10.140.67.23, enter the following:

```
# iptables -A INPUT -s 10.140.67.23 -j DROP
```

10. To remove the rule that you just added, without flushing or restoring your Linux system firewall's rules, enter `iptables -D INPUT 1` at the command line. This is assuming that the rule you added above is rule 1. If not, change the `1` to the appropriate rule number in your `iptables` command.

Chapter 26: Shifting to Clouds and Containers

1. To install and start either `podman` (for any RHEL or Fedora system) or `docker` (RHEL 7):

```
# yum install podman -y
    or
# yum install docker -y
# systemctl start docker
# systemctl enable docker
```

2. To use either `docker` or `podman` to pull this image to your host, `registry.access.redhat.com/ubi7/ubi`:

```
# podman pull registry.access.redhat.com/ubi7/ubi
            or
# docker pull registry.access.redhat.com/ubi7/ubi
```

3. To run the `ubi7/ubi` image to open a bash shell:

```
# podman run -it ubi7/ubi bash
    or
# docker run -it ubi7/ubi bash
```

4. To run commands to see the operating system on which the container is based, install the `proc-ps` package, and run a command to see the processes running inside the container:

```
bash-4.4# cat /etc/os-release | grep ^NAME
NAME="Red Hat Enterprise Linux"
bash-4.4# yum install procps -y
bash-4.4# ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 03:37 pts/0    00:00:00 bash
root        20     1  0 03:43 pts/0    00:00:00 ps -ef
bash-4.4# exit
```

5. To restart and connect to the container that you just closed using an interactive shell, enter the following:

```
# podman ps -a
CONTAINER ID  IMAGE              COMMAND   CREATED
```

```
       STATUS                    PORTS  NAMES
  eabf1fb57a3a  ...ubi8/ubi:latest bash     7 minutes ago
       Exited (0) 4 seconds ago         compassionate_hawking
# podman start -a eabf1fb57a3a
bash-4.4# exit
```

6. To create a simple Dockerfile from a `ubi7/ubi` base image, include a script named `cworks.sh` that echoes "The Container Works!", and add that script to the image so that it runs, do the following:

   a. Create and change to a new directory:

   ```
   # mkdir project
   # cd project
   ```

   b. Create a file named `Dockerfile` with the following content:

   ```
   FROM registry.access.redhat.com/ubi7/ubi-minimal
   COPY ./cworks.sh /usr/local/bin/
   CMD ["/usr/local/bin/cworks.sh"]
   ```

   c. Create a file named `cworks.sh` with the following content:

   ```
   #!/bin/bash
   set -o errexit
   set -o nounset
   set -o pipefail
   echo "The Container Works!"
   ```

7. Use `docker` or `podman` to build an image named `containerworks` from the Dockerfile that you just created.

   ```
   # podman build -t myproject .
          or
   # docker build -t myproject .
   ```

8. To gain access to a container registry, either by installing the docker-distribution package or getting an account on Quay.io or Docker Hub:

   ```
   # yum install docker-distribution -y
   # systemctl start docker-distribution
   # systemctl enable docker-distribution
   ```

   or get an account from Quay.io (`https://quay.io/plans/`) or Docker Hub, then:

   ```
   # podman login quay.io
   Username: <username>
   Password: *********
   ```

9. To tag and push a new image to a chosen container registry:

   ```
   # podman tag aa0274872f23 \
   quay.io/<user>/<imagename>:v1.0
   # podman push \
   quay.io/<user>/<imagename>:v1.0
   ```

Chapter 27: Using Linux for Cloud Computing

1. To check your computer to see if it can support KVM virtualization, enter the following:

   ```
           # cat /proc/cpuinfo | grep --color -E "vmx|svm|lm"
           flags  : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr
   pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm
   pbe syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon pebs
   bts rep_good xtopology nonstop_tsc aperfmperf pni pclmulqdq dtes64
   monitor ds_cpl vmx smx es...
           ...
   ```

   The CPU must support either vmx or svm. The lm indicates that it is a 64-bit computer.

2. To install a Linux system along with the packages needed to use it as a KVM host and, to run the Virtual Machine Manager application, do the following:

   a. Get a live or installation image from a Linux site (such as getfedora.org), and burn it to a DVD (or otherwise make it available to install).

   b. Boot the installation image, and select to install it to a hard drive.

   c. For a Fedora Workstation, after the install is complete and you have rebooted, install the following package (for different Linux distributions, you might need to install a package that provides libvirtd as well):

      ```
      # yum install virt-manager libvirt-daemon-config-network
      ```

3. To make sure that the sshd and libvirtd services are running on the system, enter the following:

   ```
   # systemctl start sshd.service
   # systemctl enable sshd.service
   # systemctl start libvirtd.service
   # systemctl enable libvirtd.service
   ```

4. Get a Linux installation ISO image that is compatible with your hypervisor, and copy it to the default directory used by Virtual Machine Manager to store images. For example, if the Fedora Workstation DVD is in the current directory, you can enter the following:

   ```
           # cp Fedora-Workstation-Live-x86_64-30-1.2.iso /var/lib/
   libvirt/images/
   ```

5. To check the settings on the default network bridge (virbr0), enter the following:

   ```
   # ip addr show virbr0
   4: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc
        noqueue state UP group default
       link/ether de:21:23:0e:2b:c1 brd ff:ff:ff:ff:ff:ff
       inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
          valid_lft forever preferred_lft forever6.
   ```

6. To install a virtual machine using the ISO image you copied earlier, do the following.
   a. Enter this command:

      ```
      # virt-manager &
      ```

   b. Select File and then select New Virtual Machine.
   c. Select Local Install Media and click Forward.
   d. Select Browse, choose the live or install ISO, click Choose Volume, and click Forward.
   e. Select memory and CPUs and click Forward.
   f. Select the size of disk that you want to use and click Forward.
   g. Select "Virtual network default: NAT" (it may already be selected).
   h. If it all looks okay, click Finish.
   i. Follow the installation process indicated by the installation ISO.
7. To make sure that you can log in to and use the virtual machine, do the following:
   a. Double-click the entry for the new virtual machine.
   b. When the viewer window appears, log in as you would normally.
8. To check that your virtual machine can connect to the Internet or other network outside of the hypervisor, do one of the following:
   a. Open a web browser, and try to connect to a website on the Internet.
   b. Open a Terminal window, enter `ping redhat.com`, and then press Ctrl+C to exit.
9. To stop the virtual machine so that it is no longer running:
   a. Right-click the entry for the VM in the virt-manager window.
   b. Select Shut Down, and then select Shut Down again.
   c. If the VM doesn't shut down immediately, you can select Force Off instead, but that is like pulling the plug out and risks data loss.
10. Start the virtual machine again so that it is running and available:
    a. Right-click the entry for the VM in the virt-manager window.
    b. Click Run.

Chapter 28: Deploying Linux to the Cloud

1. To install the genisoimage, cloud-init, qemu-img, and virt-viewer packages, enter:

   ```
   # dnf install genisoimage cloud-init qemu-img virt-viewer
   ```

2. To obtain a Fedora cloud image, go to https://getfedora.org/en/cloud/download/, and download a qcow2 image. There is one listed with OpenStack named Fedora-Cloud-Base-31-1.9.x86_64.qcow2.
3. To create a snapshot of that image in qcow2 format called myvm.qcow2, enter the following:

   ```
    # qemu-img create -f qcow2 \
   -o backing_file=Fedora-Cloud-Base-31-1.9.x86_64.qcow2 \
   myvm.qcow2
   ```

4. Create a cloud-init meta data file named meta-data that includes the following content:

   ```
   instance-id: myvm
   local-hostname: myvm.example.com
   ```

5. Create a cloud-init user data file called user-data that includes the following content:

   ```
   #cloud-config
   password: test
   chpasswd: {expire: False}
   ```

6. Run the genisoimage command to combine the meta-data and user-data files to create a mydata.iso file:

   ```
   # genisoimage -output mydata.iso -volid cidata \
       -joliet-long -rock user-data meta-data
   ```

7. Use the virt-install command to combine the myvm.qcow2 virtual machine image with the mydata.iso image to create a new virtual machine image named newvm that runs as a virtual machine on your hypervisor.

   ```
   # virt-install --import --name newvm \
      --ram 4096 --vcpus 2 \
      --disk path=myvm.qcow2,format=qcow2,bus=virtio \
      --disk path=mydata.iso,device=cdrom \
      --network network=default &
   ```

8. To open the newvm virtual machine with virt-viewer, enter the following:

   ```
   # virt-viewer newvm
   ```

9. Log into the newvm virtual machine using the fedora user and password test:

   ```
   Login: fedora
   Password: test
   ```

Chapter 29: Automating Apps and Infrastructure with Ansible

1. To install the ansible package, do the following:

   RHEL 8

   ```
   # subscription-manager repos \
       --enable ansible-2.9-for-rhel-8-x86_64-rpms
   # dnf install ansible -y
   ```

   Fedora

   ```
   # dnf install ansible -y
   ```

   Ubuntu

   ```
   $ sudo apt update
   $ sudo apt install software-properties-common
   $ sudo apt-add-repository --yes --update ppa:ansible/ansible
   $ sudo apt install ansible
   ```

2. To add sudo privileges for the user running Ansible commands, run visudo and create an entry similar to the following (changing joe to your user name):

   ```
   joe   ALL=(ALL)       NOPASSWD: ALL
   ```

3. Open a file named my_playbook.yaml, and add the following content:

   ```
   ---
   - name: Create web server
     hosts: localhost
     tasks:
     - name: Install httpd
       yum:
         name: httpd
         state: present
   ```

4. To run the my_playbook.yaml playbook in check mode, do the following. (It should fail because the user does not have privilege to install a package.)

   ```
           $ ansible-playbook -C my_playbook.yaml
           ...

           TASK [Install httpd]
   ***************************************************************
           fatal: [localhost]: FAILED! => {"changed": false, "msg":
   "This
                command has to be run under the root user.",
   "results": []}
           ...
   ```

5. Make the following changes to the `my_playbook.yaml` file:

```
---
- name: Create web server
  hosts: localhost
  become: yes
  become_method: sudo
  become_user: root
  tasks:
  - name: Install httpd
    yum:
      name: httpd
      state: present
```

6. To run the `my_playbook.yaml` file again to install the `httpd` package, enter the following:

```
$ ansible-playbook my_playbook.yaml
...
TASK [Install httpd] ***************************************
changed: [localhost]
PLAY RECAP *************************************************
localhost: ok=2 changed=1 unreachable=0 failed=0 skipped=0
rescued=0 ignored=0
```

7. Modify `my_playbook.yaml` as follows to start the `httpd` service, and set it so that it will start every time the system boots:

```
---
- name: Create web server
  hosts: localhost
  become: yes
  become_method: sudo
  become_user: root
  tasks:
  - name: Install httpd
    yum:
      name: httpd
      state: present
  - name: start httpd
    service:
      name: httpd
      state: started
```

8. To run an `ansible` command so that it checks whether or not the `httpd` service is up on `localhost`, enter the following:

```
$ ansible localhost -m service \
    -a "name=httpd state=started" --check
localhost | SUCCESS => {
```

```
"changed": false,
"name": "httpd",
"state": "started",
"status": { ...
```

9. To create an `index.html` file in the current directory that contains the text "Web server is up" and runs the `ansible` command to copy that file to the `/var/www/html` directory on `localhost`, do the following (changing joe to your user name):

```
$ echo "Web server is up" > index.html
$ ansible localhost
 -m copy -a \
   "src=./index.html dest=/var/www/html/ \
   owner=apache group=apache mode=0644" \
   -b --user joe --become-user root --become-method sudo
host01 | CHANGED => { ...
```

10. To use the `curl` command to view the contents of the file you just copied to the web server, do the following:

```
$ curl localhost
Web server is up
```

Chapter 30: Deploying Applications as Containers with Kubernetes

1. To gain access to a Minikube instance, either:

   a. Install Minikube as described here: `https://kubernetes.io/docs/tasks/tools/install-minikube`, or

   b. Access an available remote Minikube instance, such as through the Kubernetes.io tutorials: `https://kubernetes.io/docs/tutorials/`

2. To view the versions of your Minikube installation, `kubectl` client, and Kubernetes service, enter the following:

```
$ minikube version
$ kubectl version
```

3. To create a deployment that manages a pod running the `hello-node` container image, enter the following:

```
$ kubectl create deployment hello-node \
    --image=gcr.io/hello-minikube-zero-install/hello-node
```

4. To view the `hello-node` deployment and describe the deployment in detail, enter the following:

```
$ kubectl get deployment
$ kubectl describe deployment hello-node
```

5. To view the current replica set associated with your hello-node deployment, enter the following:

```
$ kubectl get rs
```

6. To scale up the hello-node deployment to three (3) replicas, enter the following:

```
$ kubectl scale deployments/hello-node --replicas=3
```

7. To expose the hello-node deployment outside of the Kubernetes cluster using LoadBalancer, enter the following:

```
$ kubectl expose deployment hello-node \
     --type=LoadBalancer --port=8080
```

8. To get the IP address of your Minikube instance and port number of the exposed hello-node service, enter the following:

```
$ minikube ip
192.168.39.150
$ kubectl describe service hello-node | grep NodePort
NodePort:                 <unset>  31302/TCP
```

9. Use the curl command to query the hello-node service, using the IP address and port number from the previous step. For example:

```
$ curl 192.168.39.105:31302
Hello World!
```

10. To delete the hello-node service and deployment and then stop the Minikube virtual machine, enter the following:

```
$ kubectl delete service hello-node
$ kubectl delete deployment hello-node
$ minikube stop
```

Index